Cyber Supply Chain Risks in Cloud Computing - The Effect of Transparency on the Risk Assessment of SaaS Applications

Olusola Akinrolabu
Kellogg College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy

Trinity 2019

Abstract

While the cloud model has many economic and functional advantages, the increased external interactions of cloud applications have expanded the complexity of its architectures and reshaped its supply chain. Due to the variety of parties involved in cloud service delivery and the high degree of supplier autonomy, assessing cloud risks has become a challenge. Also, the widespread application of traditional frameworks to cloud risk assessment has several shortcomings, including the subjectivity of risk evaluation and inability to measure cyber risk in complex systems.

Recognising that recent work on cloud risk assessment has focussed on cloud consumer risks, we sought to address the cloud service provider (CSP) risk assessment challenge. This research began with an in-depth assessment of the literature in cloud risk assessment and supply chain transparency. We conducted surveys and semi-structured interviews to validate the transparency gap and establish its link with qualitative risk assessment methods. The results of the studies substantiated the need for more rigour in cloud risk assessments and provided evidence on how this can be improved with supply chain transparency.

To address this gap, we proposed the Cyber Supply Chain Cloud Risk Assessment (CSCCRA) model; a quantitative and supply chain-inclusive model targeted at Software-as-a-Service (SaaS) CSPs. The model is made up of three main components, two of which are novel inclusions to cloud risk assessment, i.e. supply chain mapping and supplier security assessment. The CSCCRA model reflects the systems thinking approach, enabling CSPs to visualise information flow through the supply chain, assess supplier security posture, document assumptions regarding the risk factors, and appraise security controls.

In evaluating the CSCCRA model, a three-step approach was adopted. First, the developed model was evaluated by the author and members of the academic community to ensure that it met our initial criteria. Second, the model was face-validated by cloud and risk experts within the industry. Third, we conducted three real-world case studies, using the model to assess the risks of SaaS providers. The result of these evaluations confirmed the usefulness and applicability of the model for assessing cloud provider risks. Also, the case study results and subsequent development of the CSCCRA web application showed that a structured and systematic application of the proposed model within a SaaS organisation was capable of yielding objective and defensible results. The model demonstrated its utility by assisting stakeholders to quantify cloud risks, while also promoting cost-effective risk mitigation and optimal risk prioritisation.

Overall, these results advance knowledge both for research and in practice, taking us one step further into improving cloud risk assessment.

Statement of Originality

This thesis is presented in accordance with the regulations for the degree of Doctor of Philosophy. The thesis has been composed by myself and has not been submitted in any previous application for a degree. The research within this thesis was also conducted by myself. Parts of the thesis have been published or submitted as papers, and the list can be found in Section 1.7.

Acknowledgements

I give thanks to the almighty God, who is the source of all wisdom, for giving me the strength to complete this study.

I want to thank my supervisors Prof Andrew Martin and Dr Steve New, for their excellent guidance and support throughout the DPhil. Their openness to the research idea and constructive feedback played a crucial role in the successful and timely completion of this thesis.

My special gratitude goes to Prof David Wallom and Prof Felix Reed-Tsochas for their invaluable guidance through the transfer and confirmation stages. Also, I will like to thank Prof Paul Watson for accepting the request to be the external examiner for my thesis.

I want to thank my darling wife Taiwo, for her prayerful support and understanding. I will also like to thank my lovely daughter, Oluwatunmise, for always bringing joy to my heart. I must not forget my entire family for all their prayers and encouragement.

To my friend Pelumi Seweje, you were a rock of support to me through the process, and I appreciate you. Also, not forgetting my other friends and colleagues, who were a constant source of encouragement. I thank you all.

I would also like to thank the Centre for Doctoral Training (CDT) in Cybersecurity for allowing me to conduct this inter-disciplinary research. My gratitude goes to David and Maureen for their administrative and friendly support over the years. To the cohorts of CDT15, thank you for the good times we shared in our first year of study. The memory will remain with me for years to come. To other members of the CDT, thanks for making my time in the department an enjoyable one.

This research project has been possible thanks to a research grant from EPSRC (Engineering and Physical Research Council) and Kellogg College, via the CDT in Cybersecurity at the University of Oxford.

This thesis is dedicated to God
and to the memory of those I lost just before the
commencement of the DPhil and through
the course of my study.

Contents

1 Introduction **1**

1.1 Motivation . . . 1

1.2 The Problem Context . . . 4

1.3 Research Goal . . . 5

1.4 Research Questions . . . 6

1.4.1 Research Challenges and Limitation . . . 8

1.5 Research Design and Scope . . . 10

1.6 Thesis Structure . . . 11

1.7 Peer-Reviewed Publications . . . 13

1.8 Research Contributions . . . 16

2 Background **18**

2.1 Cloud Computing . . . 18

2.1.1 Cloud Delivery and Deployment Models . . . 19

2.1.1.1 Cloud Deployment Models . . . 19

2.1.1.2 Cloud Service Models . . . 20

2.1.1.3 SaaS and the API Economy . . . 21

2.1.2 Cloud Benefits and Concerns . . . 23

2.1.3 Traditional vs Cloud computing risks . . . 25

2.2 Risk Assessment Methodologies . . . 26

2.2.1 Qualitative and Quantitative Risk Assessment . . . 27

2.2.1.1 Qualitative Assessment . . . 27

2.2.1.2 Quantitative Assessment . . . 29

2.2.2 Risk Modelling . . . 30

2.3 Frameworks Referenced in our Proposed Model . . . 32

2.3.1 NIST SP 800-30 rev1 . . . 32

2.3.2 ISO/IEC 27005:2011 . . . 34

2.3.3 FAIR . . . 37

2.3.4 Summary . . . 40

2.4 Cloud Supply Chain . . . 40
2.4.1 Cloud Supply Chain Risks . . . 42
2.4.2 Transparency, Trust and Risk Assessment . . . 43
2.5 Systems Thinking . . . 45
2.6 Decision Support Analysis . . . 48
2.6.1 Z-Score . . . 49
2.6.2 Delphi Method for Information Gathering . . . 50
2.7 Summary . . . 52

3 Related Work **53**
3.1 Cloud Risk Assessment . . . 53
3.2 Conceptual Models for Assessing Cloud Provisioning Risks . . . 55
3.2.1 Existing Approaches . . . 55
3.2.2 Limitations and Gaps . . . 59

4 Research Methodology **61**
4.1 Validating the Cloud Risk Assessment Gap . . . 62
4.1.1 Cloud Supply Chain Transparency Survey and Interview . . . 63
4.1.2 Cloud Risks and Risk Assessment Survey . . . 65
4.2 Proposed Cloud Risk Assessment Approach . . . 67
4.2.1 Delphi Study for obtaining Security Factors for Supplier Assessment 72
4.2.1.1 Research Design . . . 72
4.3 Case Study for Proposed Model Validation . . . 75
4.4 Developing the Risk Assessment Web Application . . . 77
4.5 Resource Requirements . . . 79
4.6 Summary . . . 79

5 Preliminary Results and Findings **80**
5.1 Surveys and Interviews . . . 80
5.1.1 Cloud Supply Chain Transparency . . . 80
5.1.1.1 Case Study-based Survey . . . 80
5.1.1.2 Interview Results . . . 82
5.1.1.3 SaaS CSP Comparison . . . 84
5.1.2 Survey on Cloud Risk Assessment Methods . . . 86
5.1.2.1 Cloud Providers . . . 87
5.1.2.2 Cloud Customers . . . 89
5.1.2.3 General Questions . . . 90
5.1.2.4 Summary . . . 91

5.1.3 Discussion and Limitations . . . 92
5.2 Delphi Study . . . 93
5.2.1 Round One Results . . . 95
5.2.1.1 Round One Analysis . . . 96
5.2.2 Round Two Results . . . 96
5.2.2.1 Round Two Analysis . . . 97
5.2.3 Round Three Results . . . 98
5.2.3.1 Round Three Analysis . . . 99
5.2.4 Discussion and Limitations . . . 100
5.3 Summary . . . 102

6 The CSCCRA Model **103**
6.1 CSCM . . . 104
6.2 CSSA . . . 107
6.3 CQRA . . . 109
6.3.1 Combining Expert Estimates . . . 111
6.4 Summary . . . 117
6.5 Sensitivity Analysis of the CSCCRA model . . . 118
6.5.1 Experimental Design . . . 118
6.6 Expert Validation of the CSCCRA model . . . 119
6.7 Completeness comparison of the CSSCRA model with established models and standards . . . 121
6.8 Systematic evaluation of CSCCRA with other conceptual models . . . 123
6.8.1 QUIRC . . . 125
6.8.2 CSPRAM . . . 126
6.8.3 OPTIMIS . . . 127
6.8.4 Discussion and Findings . . . 130

7 Model Validation using Case Study **132**
7.1 Case Organisation One - CSP-A . . . 133
7.1.1 Background of CSP-A . . . 133
7.1.2 Application of CSCCRA to CSP-A-SaaS . . . 134
7.1.2.1 Supply Chain Mapping . . . 134
7.1.2.2 Supplier Security Assessment . . . 136
7.1.2.3 Quantitative Risk Analysis . . . 138
7.1.3 Analysis and Discussion of Assessment results . . . 143
7.1.3.1 Risk Mitigation and Treatment Recommendation . . . 145
7.1.4 CSP-A Evaluation of Model and Case Study Exercise . . . 145

7.1.5 Summary . . . 147
7.2 Case Organisation Two- CSP-B . . . 149
7.2.1 Background of CSP-B . . . 149
7.2.2 Application of CSCCRA to CSP-B-SaaS . . . 149
7.2.2.1 Supply Chain Mapping . . . 151
7.2.2.2 Supplier Security Assessment . . . 153
7.2.2.3 Quantitative Risk Analysis . . . 156
7.2.3 Analysis and Discussion of Assessment results . . . 160
7.2.3.1 Risk Mitigation and Treatment Recommendation . . . 162
7.2.4 CSP-B Evaluation of Model and Case Study Exercise . . . 164
7.2.5 Summary . . . 165
7.3 Case Organisation Three - CSP-C . . . 166
7.3.1 Background of CSP-C . . . 166
7.3.2 Application of CSCCRA to CSP-C-SaaS . . . 167
7.3.2.1 Supply Chain Mapping . . . 168
7.3.2.2 Supplier Security Assessment . . . 170
7.3.2.3 Quantitative Risk Analysis . . . 173
7.3.3 Analysis and Discussion of Assessment results . . . 177
7.3.3.1 Risk Mitigation and Treatment Recommendation . . . 181
7.3.4 CSP-C Evaluation of Model and Case Study Exercise . . . 182
7.3.5 Summary . . . 186
7.4 Case Study Summary . . . 186

8 Combined Case Study Discussion and Findings 188
8.1 Case Study Discussion . . . 188
8.2 Case Study Findings and Conclusion . . . 194
8.3 Towards a Capability Maturity Model for Cloud Risk Assessment . . . 197

9 System Development - Implementing CSCCRA as a Web Application 201
9.1 System Development . . . 201
9.2 System Evaluation . . . 206
9.2.1 Focus Group Evaluation . . . 206
9.2.2 Case Organisation Evaluation . . . 208
9.3 Summary . . . 210

10 Conclusion **211**
10.1 Introduction 211
10.2 Conclusions and Discussion 211
10.3 Limitations 216
10.4 Directions for Future Research 218
10.5 Concluding Remarks 220

Bibliography **220**

A Glossary **249**

B Coding, Description and Mapping of Security Factors **252**

C CUREC Approvals and Research Participant Invitation letters **260**

D Survey Questionnaires and Results **270**

E Assessing Cloud Risks using the CSCCRA Web Application **282**
E.1 CSP-SW-Trial Registration and Login 282
E.2 Supplier Identification and Supply Chain Mapping 283
E.3 Supplier Security Assessment 285
E.4 Risk Identification 287
E.5 Risk Analysis 287
E.6 CSP Risk Summary 290

F Sensitivity Analysis and Bounds Checking **292**
F.1 Risk Value Calculation and Sensitivity Analysis 292
F.2 Bounds Checking 305

List of Figures

1.1 Map of Research Questions 9
1.2 Research Framework for the DPhil Process 11

2.1 Separation of responsibilities between CSP and Cloud Customer. This figure has been taken from [333] 20
2.2 A typical SaaS delivery chain. This figure has been taken from [201] 23
2.3 Generic Risk Model with Key Risk Factors. This figure has been taken from [258] 30
2.4 NIST SP 800-30 Risk Assessment process. This figure has been taken from [258] 35
2.5 ISO/IEC 27005:2011 Risk Management process. This figure has been taken from [151] 36
2.6 Decomposition of Risk according to the FAIR framework. This figure has been taken from [162] 38
2.7 The essential elements of a Cloud Service 41
2.8 Transparency, Trust and Risk Management between CSP and CSC 44

3.1 Flow Diagram of Inclusion/Exclusion and Literature Analysis Process . . . 56

4.1 Research Methodology 61
4.2 Payworq service outage due to A400 ISP downtime 64
4.3 Monte Carlo Simulation Process. This figure has been taken from [276] . . 69
4.4 Conceptual view of the proposed framework 71
4.5 Iterative steps taken during the Delphi study 74
4.6 CSCCRA web application architecture overview 78

5.1 Comparison of 25 Saas Providers taken from Cloudscape 85
5.2 Risk assessment methods most commonly used within provider organisations 88
5.3 Cloud consumers' most commonly used risk assessment method for decision making 90
5.4 Hindrances to a more comprehensive risk assessment 91

5.5 CSA's top 12 cloud computing threats that are supply chain related 91
5.6 Target security dimensions for assessing cloud suppliers - Output of Delphi study 94
5.7 Representation of Participant's Industry 95
5.8 Second round Delphi security factors ratings 97

6.1 The CSCCRA Model 104
6.2 Illustration of CSCCRA risk assessment process 105
6.3 Sample Cloud Supply Chain Map 106
6.4 Cloud Supplier Security Assessment of a Sample Cloud Application 109
6.5 Schematic overview of Monte Carlo Expert estimation and Risk calculation 112
6.6 Risk value result considering security controls carried out in @RISK simulation engine 116
6.7 Risk value result without considering security controls carried out in @RISK simulation engine 116
6.8 The @RISK simulation setting used for the risk value calculation 117
6.9 Expert Validation of the CSCCRA model 121

7.1 Steps taken by case study participants using the CSCCRA model 133
7.2 Supply Chain mapping of CSP-A-SaaS using the CSCM tool 135
7.3 CSP-A's Impact Estimate vs. Risk Value Calculation 141
7.4 CSP-A Participant feedback on the CSCCRA model 148
7.5 The CSCCRA Model steps for assessing CSP-B risks 150
7.6 Supply Chain mapping of CSP-B-SaaS using the CSCM tool 152
7.7 CSP-B's Impact Estimate vs. Risk Value Calculation 160
7.8 CSP-B Participant feedback on the CSCCRA model 166
7.9 Supply Chain mapping of CSP-C-SaaS using the CSCM tool 169
7.10 CSP-C's Impact Estimate vs. Risk Value Calculation 177
7.11 CSP-C Participant feedback on the CSCCRA model 184

9.1 UML Class Diagram of the CSCCRA web application 203
9.2 Homepage of the CSCCRA web application 204
9.3 Running the web application from CLI 204
9.4 User help page for the CSCCRA web application 205

B.1 Organising the security factors into target dimensions using Affinity Diagram 253

E.1 CSP-SW User Registration and Login Page 283
E.2 CSP-SW-Trial Home Page 283

E.3 CSP-SW Pre-Assessment . . . 284
E.4 CSP-SW-SaaS Supply Chain Mapping . . . 284
E.5 CSP-SW-Trial Supplier Security Assessment . . . 286
E.6 Risk Assessment Page . . . 287
E.7 Update CSP-SW-Trial Risk Register . . . 288
E.8 CSP-SW-Trial Risk Estimation with Stakeholders . . . 289
E.9 CSP-SW Risk Summary Page . . . 291

F.1 The impact of risk factor inputs on risk value output . . . 296
F.2 Key inputs in scenario where risk value is greater than 75% . . . 296
F.3 Key inputs in scenario where risk value is greater than 90% . . . 297
F.4 Scatterplot of Risk value versus Probability of risk event . . . 297
F.5 Scatterplot of Risk value versus Impact of risk event . . . 298
F.6 Scatterplot of Risk value versus Frequency of risk event . . . 298
F.7 Spider diagram illustrating a change in impact values . . . 300
F.8 Spider diagram illustrating a change in probability values . . . 300
F.9 Spider diagram illustrating a change in frequency values . . . 302
F.10 Scatter plot showing the relationship of risk factors after frequency value change . . . 302
F.11 Spider diagram of Risk R7 . . . 303
F.12 Scatter plot of the Input variables with their correlation coefficients . . . 303
F.13 Invalid input for PwoCE_LB . . . 307
F.14 Invalid input for PwCE_ML . . . 307
F.15 Invalid input for Impact_UB . . . 308
F.16 Invalid input for Frequency . . . 308

List of Tables

1.1 Publications, submissions and contributions of authors 15

2.1 Benefits of Cloud Computing 24
2.2 Concerns of Cloud Computing 25
2.3 Traditional vs Cloud Computing Risks 26
2.4 Risk Assessment Frameworks 28

3.1 Existing Cloud Risk Assessment Models 58

5.1 Relevant demographic and cloud computing data from respondents (N = 62) 87
5.2 Round two assessment of expert consensus on security factors 97
5.3 Round three assessment of expert consensus on security factors 99

6.1 Expert Opinion Weightings 113
6.2 Experts' Estimation of Impact, Probability and Frequency of Risk 114
6.3 Combining Experts' Risk Factor Estimation based on Weightings 115
6.4 Estimated Risk Value based on Expert's estimation 115
6.5 Scoring CSCCRA's Risk identification, estimation and evaluation process using the CURF framework 124
6.6 Comparing CSCCRA's Risk identification, estimation and evaluation process with other established models. 124
6.7 CSPRAM Risk Analysis Matrix 127
6.8 Presenting a risk event with SPRAT 129
6.9 Systematic evaluation of cloud risk assessment models 129

7.1 List of Participants for Case Study One 135
7.2 CSP-A First-tier Supplier list 136
7.3 Assessing CSP-A Suppliers using CSSA 137
7.4 List of Security Risks identified by the CSP-A Stakeholders 140
7.5 CSP-A Risk Analysis result based on CQRA calculation 142
7.6 Treating CSP-A's identified risks based on Best Practice and assigning Risk Owners 146

7.7 List of Participants for Case Study Two 151
7.8 CSP-B First-tier Supplier list 151
7.9 Assessing CSP-B Suppliers using CSSA 154
7.10 List of Security Risks identified by the CSP-B Stakeholders 158
7.11 CSP-B Risk Analysis result based on CQRA calculation 159
7.12 Treating CSP-B's identified risks based on Best Practice and assigning Risk Owners 163
7.13 List of Participants for Case Study Three 168
7.14 CSP-C First-tier Supplier list 170
7.15 Assessing CSP-C Suppliers using CSSA 171
7.16 List of Security Risks identified by the CSP-C Stakeholders 175
7.17 CSP-C Risk Analysis result based on CQRA calculation 176
7.18 Assessing CSP-C's Risk using the OPTIMIS Model 178
7.19 Treating CSP-C's identified risks based on Best Practice and assigning Risk Owners 183

8.1 Cross-Case Analysis of the Three SaaS Organisations 190
8.2 Capability Maturity Model for Cloud Risk Assessment 199

9.1 CSCCRA Web Application Evaluation Questionnaire 207
9.2 Focus Group Evaluation of the Web Application 208
9.3 CSP Evaluation of the Web Application 209

B.1 Description of the 52 security criteria for Cloud Supplier Assessment 254
B.2 Description of the 52 security criteria for Cloud Supplier Assessment (contd) 255
B.3 Description of the 52 security criteria for Cloud Supplier Assessment (contd) 256
B.4 Description of the 52 security criteria for Cloud Supplier Assessment (contd) 257
B.5 Mapping of Security Factors to Standards and Guidance 258
B.6 Mapping of Security Factors to Standards and Guidance (contd) 259

F.1 Experts' Estimation of Impact, Probability and Frequency for Risk R1 . . . 293
F.2 Combined Expert Estimation of Risk R1 after five simulations of 100,000 iterations each 294
F.3 CSP-A Expert Opinion Weightings 294
F.4 Estimated Risk Value based on Combined Expert Estimates 295
F.5 Modified Experts' Estimation of Impact; Probability and Frequency unchanged 299
F.6 Modified Experts' Estimation of Probability; Impact and Frequency unchanged 300
F.7 Modified Experts' Estimation of Frequency; Impact and Probability unchanged 301
F.8 Experts' Estimation of Impact, Probability and Frequency for Risk R7 . . . 303

F.9 Criteria for conducting Input Validation and Bounds Checking 306

Abbreviations

- **API:** Application Programming Interface
- **CAIQ:** Consensus Assessments Initiative Questionnaire
- **CC:** Cloud Customer
- **CQRA:** Cloud Quantitative Risk Analysis
- **CSA:** Cloud Security Alliance
- **CSCCRA:** Cyber Supply Chain Cloud Risk Assessment
- **CSCM:** Cloud Supply Chain Mapping
- **CSP:** Cloud Service Provider
- **CSSA:** Cloud Supplier Security Assessment
- **DDoS:** Distributed Denial of Service
- **FAIR:** Factor Analysis of Information Risk
- **GDPR:** General Data Protection Regulation
- **IaaS:** Infrastructure as a Service
- **IAM:** Identity and Access Management
- **ISP:** Internet Service Provider
- **MFA:** Multi-Factor Authentication
- **MCS:** Multi-Cloud Service
- **PaaS:** Platform as a Service
- **PERT:** Program Evaluation Review Technique
- **QoS:** Quality of Service
- **RA:** Risk Assessment
- **RM:** Risk Management
- **RBAC:** Role-Based Access Control
- **SaaS:** Software as a Service
- **SMI:** Service Measurement Index
- **SPOF:** Single Point of Failure

Chapter 1

Introduction

The momentum behind cloud migrations seems to be unstoppable as organisations look to take advantage of the agility, functionality, scalability and cost benefits of the cloud. The accessibility of business and customer data through a web browser promotes increased interaction between organisations and their suppliers, customers and employees. However, against the backdrop of these cloud advantages, the rapidly evolving landscape of cyber threats means that CSPs, who provide the cloud services and the customers, who pay for and use the cloud service, often encounter challenges with assessing and estimating the value of the inherent risk of the cloud. This challenge is due to several factors, some of which include the transparency of the supply chain, visibility of security controls, the inability of traditional risk frameworks to assess risk in complex systems and the lack of sufficient resources or expertise.

In this thesis titled *Cyber Supply Chain Risks in Cloud Computing - The Effect of Transparency on the Risk Assessment of SaaS Applications*, we aim to find out the role transparency and the visibility of security controls play in the assessment of cloud risks. We focus on the development of a cloud risk assessment model and the application of the model in CSP environments, for assessing the risk of composite applications, particularly SaaS.

This chapter begins by outlining the motivation behind the study and its problem context. Then we discuss our central research question, which is made up of four subquestions, each of which contributes to the overall aim of the study. We continue by describing the general structure of the thesis, highlighting our publications and the academic contributions of this work to research and industry.

1.1 Motivation

Cloud computing is defined as a resource management model that enables convenient, on-demand access to a shared pool of computing resources [178]. It is widely believed to have changed the way Information Technology (IT) services are delivered and consumed, ushering

in disruptive technologies and introducing new business models. Cloud has grown from a promising idea to one of the fastest research and development paradigms of the computing industry. According to the Cloud Industry Forum (CIF), its ability to transform people and processes with every adoption has made it a core component of any organisation's digital transformation strategy [66].

Cloud technology is becoming more ubiquitous, and while this ubiquity gives rise to many opportunities, it also introduces new risks. According to a report by the European Union Agency for Cybersecurity (ENISA), the benefits of cloud computing, particularly its economies of scale and flexibility are both a friend and a foe [56]. Cloud services rely on a multi-tiered and often global supply chain, where services are sub-contracted based on expertise. The cloud supply chain is extraordinarily complex and highly diverse. For example, a typical Customer Relationship Management (CRM) cloud provider enlists the services of an average of eight suppliers, including application programming interface (API) and infrastructure providers, in the delivery of their application [14]. The variety of parties involved in the delivery of a cloud service widens its attack surface [44]. This new attack surface makes it possible for administrators of the CSP, cloud customers, co-tenants and external attackers to launch malicious or unintentional attacks on a cloud service. While we maintain that cloud is more secure, compared to many enterprise networks, the extent of this security is hard to verify. CSPs who should be more aware of cloud risks, find it difficult to assess their risks due to limited visibility of security controls and lack of supplier transparency [242]. This challenge has contributed to cloud risk assessment being considered as one of the most significant enterprise security weaknesses worldwide [308].

This research was motivated by a series of cloud service outages, which emphasised the impact of hidden dependencies in the supply chain of a cloud service. First was the Distributed Denial of Service (DDoS) attack on Dyn, a managed Domain Name System (DNS) infrastructure, in October 2016. This single attack almost brought down the Internet, seeing that the Dyn DNS service was relied upon by most of the popular cloud providers, e.g. Amazon, Github, Twitter and Salesforce [139]. The sole reliance of these CSPs on Dyn meant that a failure of Dyn's DNS infrastructure also meant an outage to their cloud service, with the impact felt along the chain up to 2nd, 3rd and 4th tier. The second incident was the Amazon Web Services (AWS) S3 infrastructure outage on the 28th of February, 2017. The unprecedented impact of the outage affected the global operation of a wide range of AWS customers such as Quora, IFTTT, GitHub, Slack, Netflix, Spotify and Airbnb, all of whom either experienced degradation of their cloud service or a complete service outage. Ironically, outage monitoring sites such as DownDetector and isitdownrightnow.com, which cloud stakeholders relied on for an update on their cloud services, were also offline due to their dependency on the AWS S3 infrastructure [219].

In an attempt to address the challenges of assessing cloud risks, numerous scholars have developed conceptual models [54, 58, 149, 278, 289]. While some of these studies have concentrated on cloud adoption risk assessment, others have followed the traditional route to security risk assessment, adapting the traditional risk frameworks, e.g. ISO/IEC 27005 [151], ISO/IEC 31000 [152] and NIST 800-30v1 [258]. Being predominantly qualitative or at best semi-quantitative, the prevalent use of these traditional methodologies in assessing cloud risks presents a wide range of limitations including the subjectivity of risk evaluation and the inability to cope with the dynamic cloud infrastructure [93, 309]. These frameworks were developed before the evolution of cloud computing under the assumption that an organisation's assets will be managed in-house [19]. Therefore, they are unable to cater to the complexity or pervasiveness of these automated systems of systems, often leading to increased vulnerabilities and inadequate implementation of security controls.

Furthermore, with insufficient due diligence being among the top threats of cloud computing [58], applying qualitative models which lack granularity and objectivity to assessing cloud risks is a challenging undertaking. Interestingly, the CSP transparency problem and the limited visibility into provider controls are also perceived to be contributing factors to the use of these qualitative methods [11, 242, 304]. According to Bellandi et al. [38], new approaches targeted at improving qualitative methods by accounting for the opacity of the cloud environment, have largely fallen short. This observation shows that the process of manually fitting the traditional risk assessment frameworks to address cloud risks is unsuitable.

The limitations of current risk assessment frameworks, therefore, calls for a more inclusive approach to cloud risk assessment. This approach will be one that considers the transparency[1] of the supply chain, accountability of suppliers and improves the trust of the customer. Cloud computing risk assessment requires domain-specific knowledge and a deep understanding of the Target of Assessment (ToA), i.e. cloud service, to ensure one can arrive at reasonable risk estimates. The risk landscape of a cloud service is constituted of the security risks introduced during the development, implementation, operation and maintenance phases of the service [96]; hence, with traditional frameworks, decision-making has often been based on incomplete information. Therefore, seeing that a significant novelty of cloud computing in comparison to other IT service is its dynamic supply chain, assessing the risk of a cloud service requires capturing a snapshot of its shifting landscape.

Based on the points made above, this research focuses on identifying a novel approach to assessing cloud risks, giving consideration to the interconnected nature of the cloud and the inherent risks in its supply chain. Our contribution is in the identification of gaps in cloud risk assessment, analysis of current models, and the rationalisation for the development of

quantitative and supply chain-inclusive models, targeting cloud provider risks.

1.2 The Problem Context

Assessing cloud provider risks is viewed as a significant challenge for the cloud industry [89, 99]. In multicloud systems (MCS), where cloud architectures use services from more than one CSP, the challenge of risk assessment is evident. CSPs rely on an active and complex supply chain, where the perceived level of the security risk of the cloud service increases with each additional component integrated into the offering. However, with the information security responsibility shared across the supply chain, the security posture of any CSP is potentially only as strong as the weakest member of its supply chain, particularly when their software development practices, policies, procedures, and system architecture is evaluated. For example, according to the Infosecurity magazine, due to the race to make a faster processor, the chip manufacturer Intel, had a design flaw on the chips released in 2018, which led to at least seven exploits on computing infrastructures, including Meltdown and Spectre [311].

While many of the recent academic studies (e.g., Busby et al. [54], Cayirci et al. [58] and Islam et al. [149]) have concentrated on cloud adoption/migration risk assessment, others (e.g., Sendi & Cheriet [278] and Sivasubramanian et al. [289]) have followed the traditional route to security risk assessment. This traditional approach concentrates on the focal organisation, pays little attention to the supplier network and fails to understand the interrelated consequences of the supply chain. The lack of studies targeted at the assessment of cloud service provision risks has resulted in less agile cloud environments, as described in the research works of Bartol [31], Boyens et al. [48], Johnson[159], Lewis et al. [184] and Motta et al. [209].

Furthermore, the process of selecting the best supplier for each component service, or evaluating the security risks of cloud collaborations, remains a challenge to CSPs. Some of the past studies which have proposed risk assessment model for CSPs include CSPRAM [19], OPTIMIS [89], SEBCRA [105] and QUIRC [271]. Despite best intentions, these models have many shortcomings ranging from the risk analysis method, limited scope of the assessment, expert subjectivity and inapplicability of the models in real-world scenarios.

Due to the scarcity of studies in this area and based on the practical need for cloud providers to comprehensively assess their security risks to assure customers of secure cloud delivery, it is pertinent that more research is conducted in this area. We identify the need for researchers to look into the problem of assessing cloud provider risks, with the view of improving it through the transparency of the supply chain. Also, acknowledging that the

[1]The term transparency is used in this thesis to refer to the level of documentation CSPs have on their supply chain and the ease of tracking required information clearly and efficiently.

methods of communicating cloud risks have not improved significantly in the last decade [261], we identify the need for a quantitative and data-driven process, where the value of a cloud risk is based on the decomposition of a risk scenario into its various risk variables and the risk value expressed in monetary terms.

Besides, with the architecture of a cloud service made up of software components structured as services and involving a fragmented and dispersed supply chain, assessing the risk of a cloud service requires us to understand the vulnerabilities of the individual components to identify where the weak spots exist in the supply chain.

1.3 Research Goal

This thesis aims to accomplish the following objectives: First, establish a theoretical foundation for the study regarding cloud supply chain transparency and its effect on cloud risk assessment. Second, validate the existence of these gaps with industry practitioners. Third, propose a risk assessment model that addresses the significant gaps, and, lastly, validate and improve the proposed model and implement the model into a web-based software.

Seeing that the challenge of cloud risk assessment can be traced to the application of mental models, which are arguably subjective and often leads to incorrect inferences about the security of cloud services, we plan to apply the systems thinking approach to understanding and assessing the interconnected risks of cloud systems [109, 297]. By reflecting the systems thinking method, we can develop a deep understanding of the underlying structure of a cloud system before identifying its potential risks. The primary objective of this research is to explore the potential of a quantitative and supply chain-inclusive approach to assessing cloud provisioning risks within SaaS environments. We aim to introduce novel concepts and mechanisms for improving the objectivity of cloud risk assessments from a supply chain perspective. In particular, attention will be given to developing a model, which is static but is capable of assessing the cybersecurity posture of the broader supply chain (beginning with the first tier) and assisting cloud providers in the continuous identification, analysis and evaluation of cloud risks.

A distinctive contribution of this study is that it caters for the complexities involved in the delivery of a SaaS application and has the potential to adapt to the changing nature of the cloud, enabling CSPs to conduct risk assessments at a higher frequency, in response to a change in the supply chain. Our proposed risk assessment model combines aspects of various disciplines, ranging from cybersecurity, supplier assessment, systems thinking, decision support systems, transparency, modelling, supply chain mapping and quantitative risk assessment, and applies them in a multi-staged approach to the problem area.

This research aims to advance knowledge both for research and in practice, by investigating the assessment of cloud provisioning risks which appears not to have been studied in depth. Our cloud risk assessment model will aim to provide the following:

1. A method for measuring the risk factors that constitute a cloud provisioning risk.
2. A supply chain map that identifies the degree of dependence a cloud service has on external suppliers and its potential areas of weakness.
3. A model for forecasting the risk of each supply chain member based on security factors.
4. A mathematical simulation model that estimates the risk cost based on the values of the risk factors.

Looking through the goals of our proposed model, we acknowledge that it might be challenging to make a legitimate distinction between an actual cloud risk and stakeholder's perception of the risk. This is due to factors such as the subjectivity of the humans, our inability to fully represent cloud risk as a technology property and understanding the various causes of cloud system behaviour [284]. Nevertheless, we aim to improve the assessment process through the application of a structured quantitative model capable of reducing the variation of uncertainties in risk factor estimations. Also, while it might be challenging to predict the occurrence of a cloud risk or accurately estimate its impact, our approach is to present the stakeholders with the available information on their supply chain in a format that compels them to step back from their cognitive bias [290], to enable them to make more informed estimations.

Risk perception is an inherent part of the decision-making process. However, due to the unavailability of credible information security risk data, cloud stakeholders (CSPs and customers) often result to subjective approaches to risk assessment, many of which are dependent on the stakeholder's motivational values. For example, humans have been known to underestimate risks they willingly take and overestimate risks in environments they can not control [164, 290]. As such, we aim to communicate CSP's available supply chain information (technical, process, security) using a structured model to improve the objectivity of their assessments. Seeing that the strategies for mitigating the impact of risk (actual or perceived) are often the same, our overall goal tends towards assisting CSPs to proactively mitigate the potential risks in their supply chain and consequently provide secure and reliable cloud services to their customers.

1.4 Research Questions

We have identified some of the challenges of cloud risk assessment to include the dynamic nature of the cloud infrastructure and services, the lack of physical control, the absence

of a well-structured risk management framework and the lack of trust in cloud providers [23, 309]. Also, there is a call for cloud risk assessment to move away from a qualitative and subjective approach to a more iterative, incremental and inclusive approach [54, 278].

In this study, our central research question (RQ) can be defined as *Can the transparency of the supply chain improve the objectivity of cloud risk assessment?* This central question is broken down into several subquestions as listed below, in the order in which they are addressed.

RQ1.1: What role does supply chain transparency play in assessing cloud risks?

RQ1.2: Do the existing cloud risk assessment methods adequately assess the cyber supply chain risks experienced by cloud providers and customers?

RQ2: What are appropriate reliability and security factors cloud providers can consider when choosing suppliers for the critical elements of their cloud service?

RQ3: Does the application of the supplier security assessment and cloud supply chain mapping, complement the risk assessment process, enabling SaaS cloud providers to identify their weakest suppliers, understand their cyber risks and improve the resilience of the cloud service?

RQ4: How useful is a quantitative risk assessment model, in comparison to qualitative risk assessment, in quantifying loss exposure (risk), reducing uncertainty and promoting better decision-making?

Prior academic studies have suggested that the lack of transparency is intrinsic to the operation of CSPs, and this has hindered cloud customers from assessing cloud risks [11, 242, 304]. Other industry standards reports have also argued that this same lack of transparency is a contributing factor to the predominant use of qualitative risk assessment methodologies in the cloud computing [29, 124, 112]. In Chapter 5, we validate the supply chain transparency **(RQ 1.1)** and cloud risk assessment **(RQ1.2)** gaps, using online surveys and interviews to gauge public opinion on the matter.

Recognising the limitations of existing cloud risk assessment models and their failure to address cloud provisioning risks, we propose a supply chain-inclusive, quantitative risk assessment model for the cloud. This proposed model required us to assess the cybersecurity posture of cloud suppliers while striving to understand the vulnerabilities each component supplier introduce to the cloud service. To objectively collect expert opinion on cloud supplier security rating **(RQ 2)**, we conducted a Delphi study with cloud experts to gather predictive attributes that reflect the security of a cloud supplier (see Chapters 4 & 5).

Implementing a risk assessment model without a measure of its capability does not assure its effectiveness. As such, following the development of a cloud risk assessment model, we proceeded to validate its practicality, effectiveness and usefulness, first, with academics and industry experts, and second, through the conduct of case studies with SaaS

providers **(RQ 3 & RQ 4)**. Both activities documented in Chapters 6, 7 & 8, help us to fine-tune the model, increasing its capabilities in assessing SaaS CSP risks and producing a risk assessment software (see Chapter 9). Figure 1.1 shows how the RQs feed into each other and the factors considered in each question.

1.4.1 Research Challenges and Limitation

Risk assessments are not expected to be perfect, mainly because the data upon which they are built are often inaccurate. However, we maintain that the risk assessment method should be suitable, sufficient and practicable. That said, one of the challenges we dealt with as part of the quantitative risk assessment was getting experts to efficiently estimate risk factors, without being on either side of subjective confidence (overconfident or underconfident). Another challenge was in the scoping of risk scenario to ensure that it is clear and provides sufficient information for analysis.

Due to practical constraints, a possible limitation of this study is its generalisability across all cloud service models due to the limited number of case studies conducted and the limited pool of experts with relevant experience that took part in the various stages of the project. Also, it is essential to note that our application of systems thinking to cloud computing is limited to recognising interconnections, identifying feedback (cause-effect) and gaining insight into how the supply chain structure facilitates system behaviour. Nonetheless, we believe that our theoretical propositions on the effect of supply chain transparency on cloud risk assessment hold and this can be extended to the assessment of other composite services.

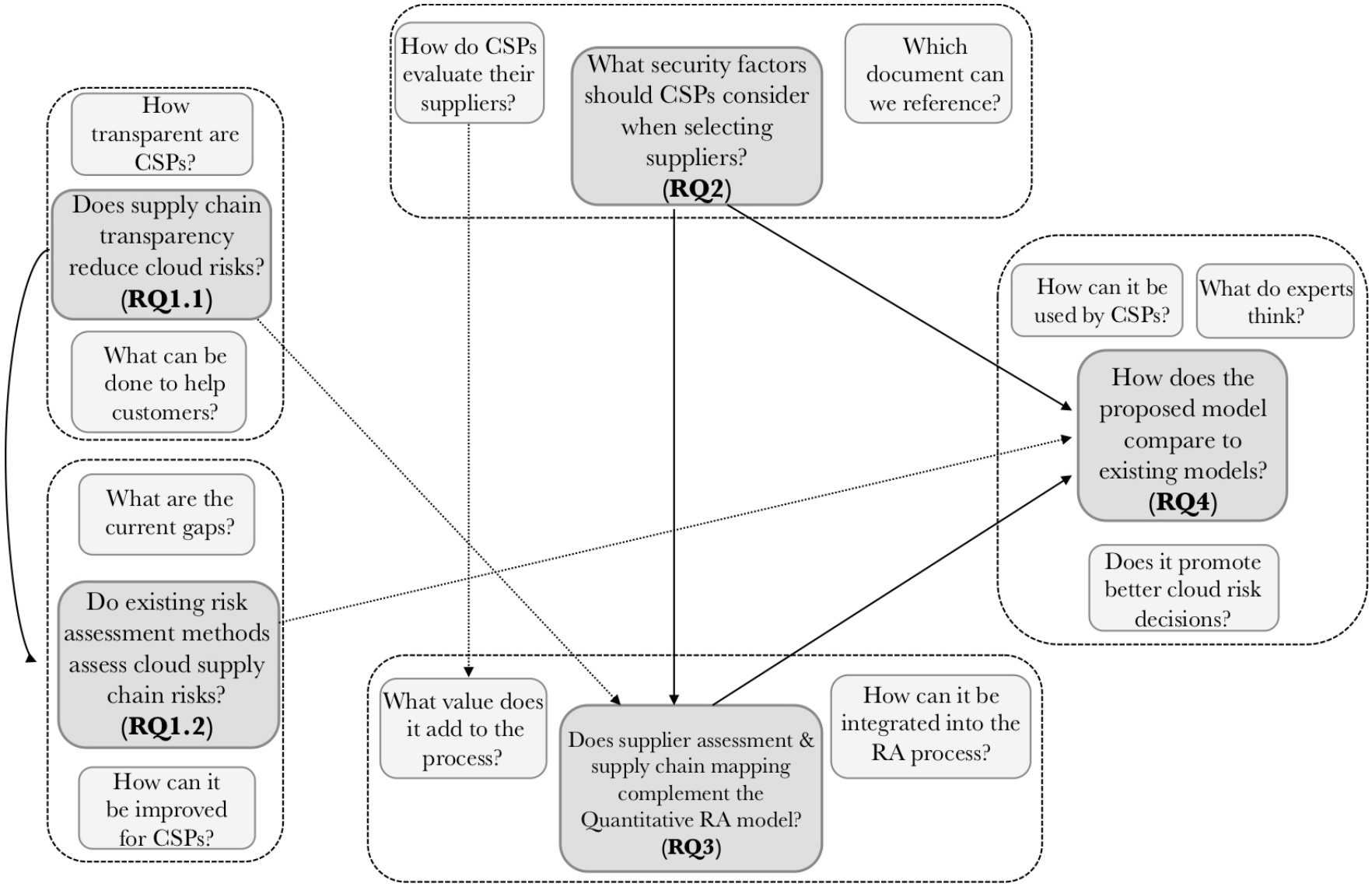


Figure 1.1: Map of Research Questions

1.5 Research Design and Scope

In this study, we aim to establish the cloud risk assessment gaps identified in literature through the use of a mixed-methods approach, including survey questionnaires and interviews. Ultimately, our goal is to improve the state-of-the-art with cloud risk assessment, by increasing the rigour involved in the process, which consequently enhances the objectivity, repeatability and reproducibility of assessment results. For this, we adopt the systems thinking approach, which gives us the ability to see the world as a complex system and understand the interconnectedness of networks [63, 108]. Applying this approach, we conceptualise and analyse the interdependencies of a cloud service, assess its risks and use modelling and simulation techniques to draw the result of the risk assessment.

Realising that our proposed model can be extended to assessing the risks of many composite services, we limit the scope of this research to assessing the cloud risks of SaaS providers. Our primary targets are SaaS providers because studies have shown that at least 80% of a typical SaaS application is made up of assembled parts, with each component representing a different level of risk [282]. SaaS applications present an excellent scope for our work, seeing that the more components combined to deliver a SaaS service, the supposed increase in the risk of the service and the higher its dependence on the supply chain. Also, recognising our inability to develop an automated model that adequately addresses the risk assessment gaps of a dynamic cloud supply chain, partly due to the time required to do so, we resolved to develop a static model capable of providing SaaS providers with a snapshot of their ever-changing cloud risks from a supply chain perspective.

Furthermore, we chose to investigate the impact of the model on cloud providers first, because we identified the advantage CSPs have over their customers concerning supply chain transparency and visibility of security controls. We hope that by analysing the application of the model within SaaS CSP environments, identifying the issues around the use of the model and providing a critically evaluated solution to those issues, we will be able to strengthen the overarching model's proposal. Likewise, the results of this study, if positive, can inform the need for improved cloud transparency, which will promote better cloud risk assessment and help CSPs and customers, develop and use secure cloud services.

This research follows an action design approach, where we design a framework for assessing cloud risks, validate its use with experts and progress to apply it in a real-world context. The case study is conducted to validate if the structured and systematic application of our proposed model within SaaS organisations yields objective and defensible risk assessment results. Although to properly evaluate this proposed model, we require CSPs to gather comprehensive information on their suppliers as part of the supplier security assessment. We believe this will take considerable time and require supplier cooperation. Considering

this limitation, we confine the validation case studies to the information CSPs already have about their suppliers and other publicly available information.

While the case studies conducted as part of this study are not the primary goal of the research, they provide a workbench for us to improve the proposed model, evaluate its usefulness, validate its applicability and test our methods.

1.6 Thesis Structure

This thesis applies the Design Science Research (DSR) [321] to address unsolved research problems in the cloud industry, i.e. proposing and implementing a practical and useful approach for assessing cloud provisioning risks. The research carried out as part of this thesis is structured as shown in Figure 1.2.

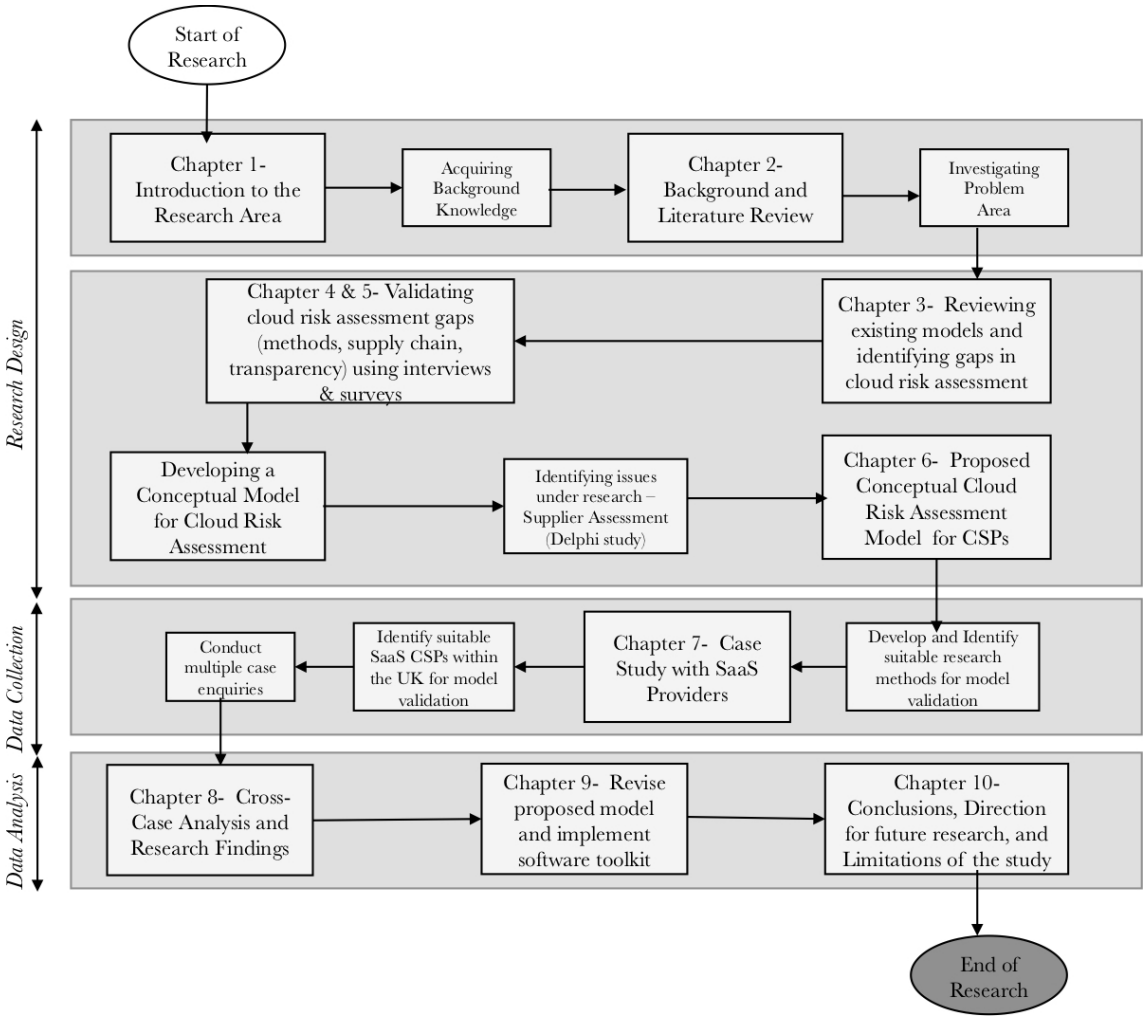


Figure 1.2: Research Framework for the DPhil Process

We will now outline the contents of each chapter, which is based on the studies undertaken and follows a coherent narrative, with each study informing the subsequent phase.

1. In Chapter 2, we provide background information on the different body of knowledge applied in a multi-staged approach to the problem area. We begin with cloud computing, describing its models and highlighting its benefits and concerns. Next, we discuss three of the risk assessment frameworks referenced in the development of our proposed cloud model. Following this, we considered the cloud supply chain, the role of transparency and trust in risk assessment, systems thinking and decision support analysis.

2. Chapter 3 presents a review of the state-of-the-art in cloud risk assessment. Owing to the scarcity of models targeted at cloud provisioning risk assessment, we conducted a three-staged literature review to identify conceptual models that are applicable to cloud provider environments, justifying our selection with a set of criteria. Finally, we conclude the chapter by highlighting the limitations of existing approaches and outlining our approach to addressing the identified gaps.

3. In Chapter 4, we detail the design of the four studies conducted to address our central research question. We highlight how each study was undertaken, describing its population, research instrument and data collection procedures. For each study, we justify the selection of the quantitative or qualitative research method. Also, we introduce our proposed risk assessment model and describe the Delphi study conducted to address the supplier security assessment element of the model. Finally, we describe the case study method, developed to validate the applicability of our work in real-world scenarios.

4. Chapter 5 presents the results of our surveys, interviews and Delphi study. Here, we validated the cloud supply chain transparency and cloud risk assessment gaps identified in the extant literature. The results of the survey linked the cloud risk assessment challenge to the lack of cloud provider transparency. Also, in this chapter, we present and analyse the result of our online Delphi study, where experts achieved consensus on a total of 52 security criteria for comparing the security of cloud vendors. The results presented in this chapter, provide answers to research questions **RQ1.1**, **RQ1.2** and **RQ2**.

5. Chapter 6 presents the CSCCRA model, proposed to assist CSPs in assessing their cloud service risks. The quantitative risk assessment model whose aim is to objectively present stakeholders with an understanding of their cloud risks is made up of three components: cloud supply chain mapping (CSCM), cloud supplier security assessment (CSSA) and cloud quantitative risk analysis (CQRA). We describe how each component is used in the different phases of the risk assessment and the improvements of this

model on existing methods. Furthermore, we conducted a sensitivity analysis of the model, carried out a completeness comparison of the model with international standards and systematically evaluated it with three other established conceptual models to illustrate its novelty. Lastly, we present the result of face-validation of the model's proposal by ten cloud and risk experts.

6. In Chapter 7, we demonstrate the applicability and usefulness of the model in assessing cloud provider risks by validating its use within a real-world context. The case study is limited to three small and medium SaaS CSPs. Using the model, participants decompose each cloud service into its constituent elements, draw out its supply chain, assess its supplier's security and estimate the value of the identified risks. We present the result of the detailed evaluation of the model's proposal within these organisation and their suggestions for future improvement.

7. Chapter 8 presents the cross-case analysis of the three case studies conducted in Chapter 7. Here, we discuss the similarities and differences in the case organisations and extract the important findings from the use of the model in these CSP environments. Also, in this chapter, we provide answers to research questions **RQ3** & **RQ4**.

8. Chapter 9 presents a web-based implementation of the CSCCRA model. Following the feedback from case studies, we refined certain aspects of the model's operation, making it easily accessible and intuitive to cloud stakeholders. We present the result of the model's practical evaluation with our focus group and a previous case organisation.

9. Chapter 10 concludes the thesis and summarises the research project. We discuss the key findings of our research and demonstrate the answers to our research question. The chapter continues by identifying the limitations of our study and outlining future research directions that could advance the ideas embodied in this work.

1.7 Peer-Reviewed Publications

We present the research published during the DPhil that relates to the content of this thesis and link it to the relevant chapters. Seven articles that relate to the DPhil topic have been published. However, one of them is an extended journal article. This article [16] extends the work presented at the EMCIS conference [13], and in it, we provide a more detailed description of the CSCCRA model, compare the completeness of the model with other established methods and use the model to assess the risks of a real-world SaaS application.

Our peer-reviewed publications are as follows:

- Akinrolabu O. and New S., *Can Improved Transparency Reduce Supply Chain Risks in Cloud Computing?*, Proceedings of the 7th International Conference on Operations and Supply Chain Managemen (OSCM), 2016 (This paper forms the basis of Chapters 4 & 5).

- Akinrolabu, O., New, S. and Martin, A., *Cyber Supply Chain Risks in Cloud Computing-Bridging the Risk Assessment Gap*, Open Journal of Cloud Computing (OJCC), Volume 5, Issue 1, pp. 1-19, 2018. (This paper forms the basis of Chapters 4 & 5).

- Akinrolabu, O., New, S. and Martin, A., *CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers*, Proceedings of the 15th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS),2018 (pages 177-184). Springer Lecture Notes in Business Information Processing. (This paper forms the basis of Chapters 4 & 6).

- Akinrolabu, O., New, S. and Martin, A., *Cloud Service Supplier Assessment: A Delphi Study*, Proceedings of the 8th International Conference on Innovative Computing Technology (INTECH), 2018, pages 142-150. (This paper forms the basis of Chapters 4 & 5).

- Akinrolabu, O., New, S. and Martin, A., *Assessing the security risks of multicloud SaaS Applications: A Real-world case study*, Proceedings of the 6th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2019), 2019, pages 81-88. (This paper forms the basis of Chapter 7).

- Akinrolabu, O., Nurse, J., Martin, A., New, S., *Cyber risk assessment in cloud provider environments: Current models and future needs,* Computers & Security Journal, Volume 87, pp. 1-18, 2019. (This paper forms the basis of Chapters 4, 6 & 7).

- Akinrolabu, O., New, S., Martin, A. *CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers,* Computers Journal, Volume 8, Issue 3, pp. 1-17, 2019. (This paper forms the basis of Chapters 4, 6 & 7).

Also, in the course of the DPhil, we published a conference paper on the detection of sophisticated attacks in Security Operations Centers (SOCs) [9] and was a guest author for the British Computer Society (BCS) magazine issue on cloud computing. The article was titled "*Assessing cloud risk: The supply chain perspective*" [10].

All publications that relate to the content of this thesis are presented in Table 1.1, with my contribution to papers with multiple authors described. In each of the published articles, I was the first author and was responsible for the research reported and writing the original manuscript, with contributions from the other authors.

Table 1.1: Publications, submissions and contributions of authors

Venue	**Publication/Submission**	**Authors Contribution**
Proceedings of the 7th International Conference on Operations and Supply Chain Management (OSCM), 2016. OSCM Journal, 10(3) pp. 130-140	Conference paper - Akinrolabu O. and New S., *Can Improved Transparency Reduce Supply Chain Risks in Cloud Computing?* (this paper forms the basis of Chapters 4 & 5)	O.A conceived the original idea. O.A and S.N contributed to the design of the research. O.A conducted the research and wrote the draft paper. S.N supervised the work .Both O.A and S.N reviewed and edited the paper
Open Journal of Cloud Computing (OJCC), Volume 5, Issue 1, pp. 1 -19, 2018	Journal article: Akinrolabu, O., New, S. and Martin, A., *Cyber Supply Chain Risks in Cloud Computing- Bridging the Risk Assessment Gap* (this paper forms the basis of Chapters 4 & 5)	O.A conceived, planned and conducted the study. O.A wrote the paper with editing and review inputs from other authors. A.M and S.N were involved in the planning and supervision of the work
Proceedings of the 15th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS), 2018 (pages 177-184). Springer Lecture Notes in Business Information Processing	Conference paper: Akinrolabu, O., New, S. and Martin, A., *CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers* (this paper forms the basis of Chapters 4 & 6)	O.A conceived the idea, designed the model, and wrote the original paper. A.M and S.N supervised the work and provided critical feedback which helped to shape the research, analysis and article
Proceedings of the 8th International Conference on Innovative Computing Technology (INTECH), 2018, pages 142-150	Conference paper: Akinrolabu, O., New, S. and Martin, A., *Cloud Service Supplier Assessment: A Delphi Study* (this paper forms the basis of Chapters 4 & 5)	O.A conceived, planned and conducted the study. O.A wrote the paper with editing and review inputs from other authors. A.M and S.N were involved in the planning and supervision of the work
Proceedings of the 6th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2019), 2019, pages 81-88	Conference paper: Akinrolabu, O., New, S. and Martin, A., *Assessing the security risks of multicloud SaaS Applications: A Real-world case study* (this paper forms the basis of Chapter 7)	O.A conceived, planned and conducted the study. O.A wrote the paper with editing and review inputs from other authors. A.M and S.N were involved in the planning and supervision of the work
Computers & Security Journal, Volume 87, pp. 1 - 18 2019	Journal article: Akinrolabu, O., Nurse, J., Martin, A., New, S., *Cyber risk assessment in cloud provider environments: Current models and future needs* (this paper forms the basis of Chapters 4, 6 & 7)	O.A conceived, planned and conducted the study. O.A wrote the paper. J.N reviewed and edited the paper. All authors contributed to the final version of the article. A.M and S.N supervised the project
Computers Journal, Volume 8, Issue 3, pp. 1 - 17, 2019	Journal article: Akinrolabu, O., New, S., Martin, A., *(Extended paper) CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers* (this paper forms the basis of Chapters 4, 6 & 7)	O.A conceived the idea, designed the model, and wrote the original paper. A.M and S.N supervised the work and provided critical feedback which helped to shape the research, analysis and article

1.8 Research Contributions

These are the areas we believe the work presented in this thesis, has contributed to the area of cloud provider risk assessment and extended the boundaries of knowledge. The individual elements of the contributions made by our work stem from different components in this thesis, directly align with our research questions and have been published. Our contributions include the identification and validation of the supply chain transparency gap in cloud risk assessment reported in Chapters 3, 4, & 5, the proposal of a supply chain-inclusive risk assessment model as contained in Chapter 6 and the validation of the model's applicability to SaaS provider environments in Chapter 7. Our proposed model (CSCCRA), is to our knowledge, the first quantitative cloud risk assessment model that addresses the effect of the supply chain transparency on cloud risks. Despite its static nature, the model's approach enables CSPs to capture a snapshot of their dynamic cloud supply chain and illuminates the perceived risks of the cloud service to decision-makers. This thesis also demonstrates a contribution to research through the rigorous testing of the viability of the CSCCRA model for improving cloud risk assessment.

A summary of our contributions to both theory and practice is as follows:

1. In Chapter 5, we contribute to the body of knowledge, by validating the cloud supply chain transparency gap and its connection to qualitative risk assessment methodologies. We show, through a mixed-method study, the general opaqueness of CSPs and how the lack of visibility of implemented security controls, constrain cloud consumers to carry out qualitative and subjective assessments of their cloud risks. Through the studies, we identified eight (8) transparency features, which we believe CSPs can share with their customers, to build trust and reduce perceived risk, without impeding on their competitive advantage or violating their intellectual rights.

2. In Chapter 5, we contribute security criteria which can be used by CSPs in rating and comparing the cybersecurity posture of their vendors. This study was conducted due to the lack of a widely accepted framework or standard for cloud supplier security assessment, which has led many cloud stakeholders to implement a distorted and often incomplete supplier assessment. We achieved these criteria through a Delphi study, where experts reached consensus on 52 security criteria grouped into nine (9) target security dimensions. These findings do not only contribute to improving cloud provider risk assessment, but they also provide cloud customers with a concise list of security criteria to consider when selecting providers. Through the case studies, we confirmed that these security factors possess high predictive validity in assessing the cyber posture of cloud suppliers.

3. In Chapter 6, we contribute a formalised model for the assessment of cloud provider risks. The Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, is a quantitative model which is supported by the CSSA, CSCM and CQRA tools. Both the CSSA and CSCM are novel integrations into a cloud risk assessment model. We introduced the CSCM to enable risk assessors to visualise the cloud service through the lens of its supply chain, identifying its vulnerabilities, hidden dependencies and critical suppliers. Likewise, the CSSA allows the CSP to assess the cybersecurity posture of cloud suppliers before the risk identification phase. The novelty of the CSCCRA is that it is an effective and efficient cloud risk assessment framework which provides visibility into the supply chain and supports comprehensive risk identification, analysis, evaluation and a cost-benefit analysis for security control implementation.

4. In Chapter 7, we establish a relationship between preliminary assessment activities and the increased objectivity in stakeholder estimations during cloud risk assessment exercises. Using three case study exercises, we confirmed the extent to which the use of a decision support system (i.e. CSCM and CSSA) affords CSPs the opportunity to learn more about the supplier's security controls (management, operational and technical) and the potential vulnerabilities in their SaaS application, based on security gaps in the supply chain. The application of the quantitative model suggested that despite the lack of historical data, CSPs could improve the objectivity of their cloud risk assessments through the use of controlled experimentation, clearly defined model, expert calibration and supply chain visibility.

Chapter 2

Background

In this chapter, we take an in-depth look into the different knowledge areas related to our work, to lay a foundation for the rest of the thesis. We review background in areas such as cloud computing, risk assessment, cloud supply chain, transparency, systems thinking and decision support analysis.

2.1 Cloud Computing

Over the years, numerous definitions have been given for cloud computing [183, 291, 332]; many of which have highlighted the various benefits of the IT deployment model. However, researchers have broadly adopted the National Institute of Standards and Technology (NIST) definition, which identifies the five essential characteristics of the cloud. According to NIST [291], cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In its purest sense, cloud computing is a computing resource management model. It is a method for pooling and distributing hardware infrastructure resources on a massive scale [179]. Cloud computing is composed of five essential characteristics, three service models and four deployment models. The commoditisation of cloud computing has resulted in a radical form of vertical disintegration where the physical infrastructure is unbundled from the platform layer and offered as a service [179]. It lowers the entrance barrier to service provision, especially for small and medium businesses (SMBs), who now have access to compute-intensive applications, hardware resources with no upfront cost, a platform for innovation and IT scalability [197].

The five essential characteristics of cloud computing are as follows [29]:

- **Broad network access:** Access to cloud resources is available over a range of device types ranging from thin to thick client platforms, e.g. mobile phones, tablets, laptops and workstations.

- **On-demand self-service:** The cloud architecture provides an illusion of infinite resources being made available to the user, and it enables users to efficiently provision computing resources, such as a server, network or storage capability, without requiring human interaction or assistance of the service provider.

- **Resource pooling:** The provider's computing, network and storage resources are pooled to serve multiple customers. These resources (physical, virtual) are dynamically assigned and reassigned according to customer demand.

- **Measured service:** In a similar fashion to how users are charged for utilities (e.g. gas), the use of pooled resources in the cloud are monitored and reported to the customer, providing them visibility of their consumption, a rate for the service and total cost.

- **Rapid elasticity:** Rapid elasticity is the ability to scale outward or inward commensurate with demand. This characteristic has the potential of reducing IT costs since the majority of the costs associated with deploying applications stems from provisioning (moves, adds and changes) in the cloud supply chain [329].

2.1.1 Cloud Delivery and Deployment Models

Cloud computing employs a service-driven business model and is typically classified based on its delivery or deployment models. The details of the business requirements, drive the choice of cloud deployment model and its architecture.

2.1.1.1 Cloud Deployment Models

There are four cloud deployment models (private, public, community and hybrid) and each present particular trade-offs in the cloud customer's control of their cloud resources, the scalability of the cloud infrastructure and the availability of cloud resources [29]. A brief description of each cloud models is as follows:

1. **Private cloud:** The private cloud is made up of services that have been pooled together and provisioned for a single organisation's use. The organisation's internal IT team could manage it, or it could be outsourced to a third-party. Similarly, the private cloud could be on-premise or off-premise, but its resources are dedicated to the use of a single entity [154, 168].

2. **Public cloud:** Here, the cloud hosting infrastructure is provisioned for use by the general public. This model embraces the tenets of cloud computing, including measured service, rapid elasticity and multi-tenancy. The public cloud is typically based on a pay-per-use model, similar to the prepaid electricity metering system, and it is

flexible through periods of varied consumption. However, public clouds are perceived to be less secure, when compared with other models and customers are required to do more to protect their data from malicious attacks [154].

3. **Community Cloud:** The community cloud infrastructure is provisioned for exclusive use by a specific community of consumers, whose organisations share a mutual concern (e.g. research or security requirements) [29]. A community cloud may be managed by a third party or by members of the community.

4. **Hybrid cloud:** A hybrid cloud is a composition of two or more distinct cloud infrastructures (public, private, or community), that form a new entity, unique in its operation, but bound together by standardised or proprietary technology for data and application portability [29]. Nevertheless, the hybrid cloud could be prone to data integration problems such as data quality control, security issues and lack of mechanisms to detect changes to data [34].

2.1.1.2 Cloud Service Models

Cloud computing enabled the provision of hardware and platform level resources, providing cloud resources 'as a service' and on-demand [335]. Based on some level of abstraction, a cloud service is presented to an end-user as one of the three service models, namely, Software-as-a-Service(SaaS), Platform-as-a-Service(PaaS) or Infrastructure-as-a-Service(IaaS). The responsibility distribution between the CSP and customer for each of the cloud service models is as shown in Figure 2.1.

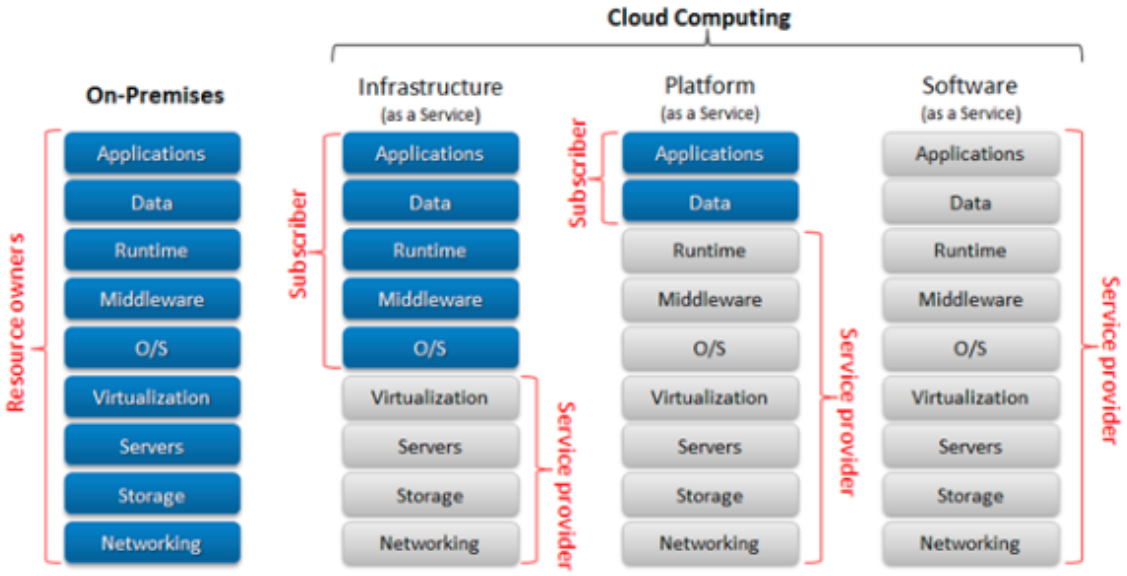


Figure 2.1: Separation of responsibilities between CSP and Cloud Customer. This figure has been taken from [333]

1. **IaaS -** The IaaS service model is the foundation of all cloud services as it presents customers with virtualised resources (storage, servers and network) on which they can run their operating system and build their application stack [2]. The customer does not control the underlying physical infrastructure but can launch virtual machines and install operating systems, which is then managed by the cloud customer. Regarding security, the IaaS service provider typically only provides basic levels of security around the perimeter of the customer's infrastructure, leaving the customer with the responsibility of providing host-based security to protect their cloud applications [299].

2. **PaaS -** The PaaS service model refers to the delivery of a computing platform and solution stack as a service [299]. PaaS abstracts every underlying infrastructure up to the middleware level and offers developers, resources and tools with which they can build and manage their applications. A PaaS service often takes advantage of the virtualisation capabilities of the IaaS model, but in the same way that it inherits the capabilities of the underlying infrastructure, it also inherits the security issues and risks [299].

3. **SaaS -** SaaS is a model of software deployment whereby a CSP licenses an application to customers for use as a service on demand [299]. The SaaS CSP license the applications to customers either as an on-demand pay-as-you-go service or at no charge. SaaS applications are accessed using web browsers over the Internet or through a client application installed on the end-user device, with most of the application program logic executed on the CSP's servers [29]. In a SaaS model, the customer does not manage the underlying infrastructure, and they only have limited access to user-specific application configuration settings [29].

2.1.1.3 SaaS and the API Economy

Cloud computing is referred to as a disruptive technology, and the SaaS model is known to have disrupted the independent software vendor landscape [39]. Applications such as Adobe Photoshop, which were delivered to customers locally as a desktop software, are now reliably accessed over the Internet, without the customer making any direct investment in infrastructure. According to Forbes, SaaS is the early winner in the cloud space, accounting for the largest revenue share of the three cloud models [69]. In SaaS, customers depend on their provider for adequate security measures, including data security, network security, data segregation, vulnerability management and configuration management. The customers relinquish their control over the software versions or changing requirements and maintain limited admin control and user level control. SaaS clouds provide scalability and shifts burdens from consumers to providers, in the process creating new opportunities for

greater efficiency and performance. Also, the SaaS eliminates the up-front cost of equipment acquisition but requires a potentially recurring usage fee [29].

Although the SaaS model is the most visible to end-users, it is often made up of a mesh of components, which appears as a single service to the consumer. The components of a SaaS application, are made up of loosely coupled services, which helps to promote the interoperability and federation between different cloud environments [238]. SaaS customers are not always aware of the underlying platforms, infrastructure, or hardware, and this lack of visibility increases security, compliance and data mobility concerns. The primary concern for the SaaS model is often security, seeing that it require organisations entrusting their sensitive information and processes to a third-party service provider, who might also rely on other suppliers, all with their security challenges.

The growth in cloud computing technologies has encouraged SaaS providers to leverage already manufactured services (e.g. API) in building their cloud services. This single action has reduced the entry barrier to cloud service provisioning. The use of API is crucial to the process of unlocking IT innovation and is often referred to as the glue of cloud computing. This reputation is beyond the hype, considering Gartner also forecasted a 20% compound annual growth for APIs through to 2017 [171]. However, the root cause of a majority of cloud security attacks has been traced to poor quality APIs or inadequate testing during application development [67, 68]. Developers in failing to prioritise security while building or re-using APIs, have put both application and underlying data at risk of overexposure and attack [68].

Sandoval [268] suggests that to identify the penalties of vulnerabilities in cloud applications, API providers should compare an entire IT system to a person girded with armour including plates, spines and reinforcing braces, but lacks a simple gorget to protect the throat, making the person vulnerable to a single blow. With any application or system involving the integration of multiple functionalities provided by a complex supply chain, the system can only be considered as secure as its weakest part. The concept of the weakest link in a supply chain further highlights the interdependence of cloud computing risks, where although individual systems can be secure in isolation, they can quickly become insecure when combined, whether due to application syntax, feature interaction, slow information leakage or concurrency problems [177]. Malicious actors only need to attack the weakest link in the chain to cause an outage for the entire system.

In conclusion, the security and reliability of the SaaS model is a function of its development process. Seeing that cybersecurity never gets solved 100%, irrespective of the level of innovation, mitigating cloud and API risks should lean towards process-based solutions. Organisations integrating API services into their SaaS applications need to have a strategy

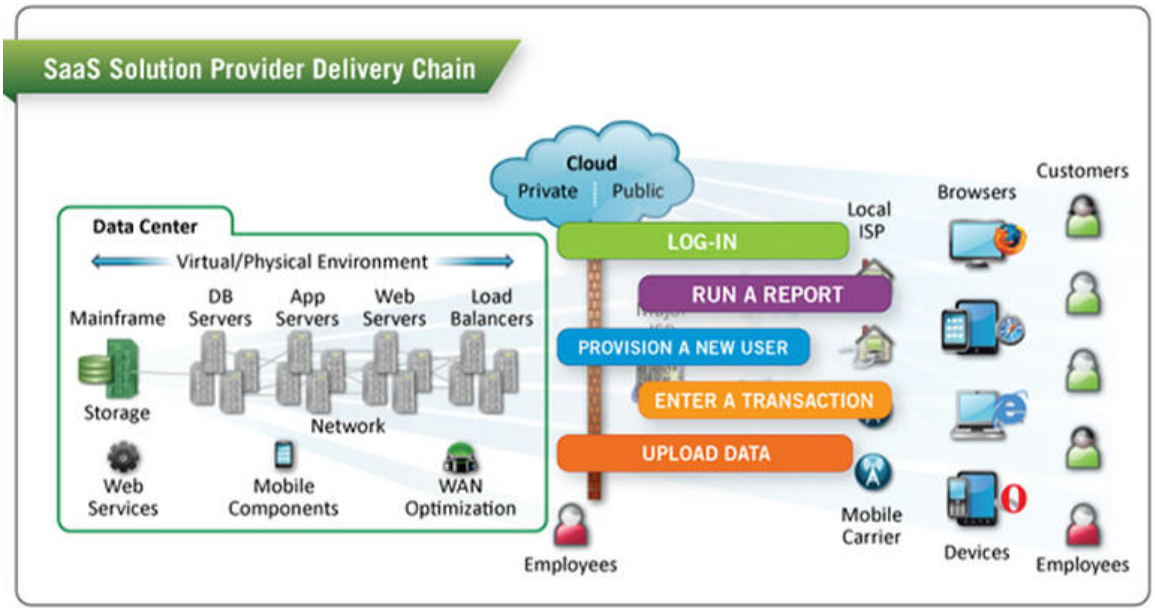


Figure 2.2: A typical SaaS delivery chain. This figure has been taken from [201]

on how to evaluate application security and mitigate the risks posed by APIs, including loss of integrity, confidentiality and availability of data.

2.1.2 Cloud Benefits and Concerns

It has been widely suggested that cloud technology is the future of computing [262], seeing that its incredible pace of development has resulted in several technological innovations. While the benefits of using cloud services are well defined, the deliberation about the challenges that may frustrate the seamless adoption of these services remains open for discussion. There is a large number of published academic (e.g. [23] and [336]) and industry (e.g. [148]) studies that describe the benefits of cloud computing. However, in all of these studies, security and privacy are still perceived to be the primary obstacles to the broad adoption of cloud computing, especially the public cloud [154, 279]. Security concerns exist at every layer of the cloud model. Joshi et al. [163] discussed different types of threats related to IaaS and suggested methods to mitigate them. The authors dealt with IaaS issues specifically because such issues if unresolved can be harmful to the entire cloud infrastructure. PaaS related attacks include media access control (MAC) spoofing and exploited scripts, and the SaaS layer can get affected due to attacks on APIs.

The benefits of cloud computing can be addressed from three main categories, which are: economic, technical and usability [194]. These benefits can also be discussed from the perspective of the service model or size of the organisation. According to a study conducted by the Information Systems Audit and Control Association (ISACA) & Cloud Security Alliance (CSA) [148], preference for performance-improvement benefits seems to correlate

to SaaS adoption by SMBs, but the preference for financial benefits correlates with the rate of IaaS and PaaS adoption by large enterprises. Contrary to the established premise for the abstraction and centralisation of computing resources through cloud computing, ENISA [85] argue that this could result in a 'double-edged sword' situation. On the one hand, large cloud providers can deploy state-of-the-art security and resilience solutions, while on the other, an outage or security breach could be significant, impacting many businesses and end-users. The increased numbers of parties, devices and applications involved in cloud service delivery, leads to an increase in attack surface and consequentially an increased threat of data compromise [337].

In our review of existing literature computing, including comments from industry experts [191], we present a summary of the benefits and concerns of cloud computing in the Tables 2.1 & 2.2 below:

Table 2.1: Benefits of Cloud Computing

No.	Cloud Benefit	Authors
1	Cost effectiveness through pay-per-use model (utility charging), OPEX vs CAPEX	[183],[336],[113],[59],[256], [5],[337],[148],[29]
2	Economies of scale through volume operations and resource concentration	[336],,[320], [183]
3	Rapid scalability of infrastructure and capacity planning	[113],[59], [256], [337],[320],[148],[5]
4	Performance benefit (security, service availability, and compliance obligations)	[337],[59],[148],[5]
5	Decreased customer effort in managing technology through access to providers' expertise and skills	[5],[59], [29],[320], [336],[256]
6	Speed of deployment through componentisation	[59], [256], [336], [320]
7	Location independence	[337],[113]
8	Flexibility/Elasticity of cloud resources	[337],[183],[148]
9	Cloud reliability improves through the use of multiple redundant sites	[337],[320],[336]
10	Business Agility and Innovation	[100],[203],[148],[121]

Based on users perception of the contents of Tables 2.1 & 2.2, it would seem that cloud concerns, e.g. security, loss of governance and vendor lock-in, outweigh cloud benefits, e.g. cost-effectiveness, flexibility and rapid scalability. While these concerns, particularly the security and privacy ones, have been known to hinder the widespread adoption of cloud computing, we argue that cloud benefits outweigh its risk. This is because, despite the imperfections of the cloud, only a few organisations have experienced cloud issues that would force them out of the cloud and back to their private datacentres. Cloud computing does not just lead to greater efficiency and economic benefits; it also improves the security of corporate networks. For many organisations, especially SMBs, the cloud has offered them access to the expertise they would otherwise be unable to afford, which has gone on to improve their business and process performance and security posture [35, 179].

Table 2.2: Concerns of Cloud Computing

No.	Cloud concern	Authors
1	Security concerns	[336], [59],[256],[242],[154],[148],[279]
2	Privacy and access control concerns	[336],[59],[256],[242], [304],[154],[279]
3	Compliance concerns,(jurisdiction and , regulation, legal, forensic support)	[59], [304],[29],[154],[230],[191]
4	Contract lock-in, hidden costs	[148],[59], [5],[209],[154],[98],[91]
5	Insecure or incomplete data deletion/ Risk of data leakage	[59], [29],[279],[154],[191]
6	High-value cyber-attack targets/ Multi-tenancy issues	[59], [256],[5],[29]
7	IT Organisational changes	[59], [336],[5]
8	Security or Isolation failure/ Availability issues	[98], [84],[230] ,[91]
9	Data/Resource location	[256],[29],[154],[279],[304],[59]
10	Lack of transparency and visibility of control	[242], [304],[29],[279],[241],[174]
11	Loss of governance	[29],[101],[230],[191]
12	Lack of a well-defined supply chain	[29],[188],[84]
13	Cloud reliability - complexity of cloud applications	[29],[209],[5],[59]
14	Lack of trust in CSP	[279],[154],[241],[174],[91],[191]
15	SLA deviation	[212],[279],[29],[209]
16	Interoperability and portability issues	[192],[209],[29],[84],[192],[238]

Therefore, cloud customers are encouraged to explore the trade-offs between cloud benefits and concerns quantitatively. Each organisation needs to be sure that the economic savings of cloud adoption are not wiped away by its potential security, complexity and compliance overheads.

2.1.3 Traditional vs Cloud computing risks

Cloud computing is often associated with the public cloud, which promotes the outsourcing of all or part of an organisation's computing environment to an external CSP. The cloud provides IT-related capabilities as a service, accessible primarily via a web browser, requiring limited knowledge of the underlying technologies and with minimal management effort. Knowing that the cloud inherits the risk of its underlying architecture, including virtualisation and the Internet, it is faced with the challenge of solving the security concerns of the traditional datacentres, coupled with dealing with the new issues inherently introduced by the cloud computing paradigm itself [156, 256]. That is, the cloud adds a 'delta' to traditional security issues. According to the Committee of Sponsoring Organisations (COSO) [59], typical cloud computing risks include disruptive force, multi-tenancy, lack of transparency, performance and reliability issues, vendor lock-in, security and compliance concerns, many of which were not evident under the traditional computing model.

Table 2.3 presents a comparison of how traditional computing risks differ from public cloud computing risks.

Table 2.3: Traditional vs Cloud Computing Risks

Criteria	Traditional Computing Risk	Cloud Computing Risk (Public)
Multi Tenancy	Implements the physical separation of controls, when IT resources need to be shared by multiple customers.	A complicated system of resource sharing. Places greater dependence on logical separation at multiple layers of the application stack.
Loss of Control	Organisation remain in control of data and decide where it is stored and how it is used.	With the possibility of data stored in multiple datacentres, coupled with the lack of visibility of CSP controls, customers would seem not to be in control of their data.
Access Control	The security perimeter acts as the trust boundary where sensitive information is stored and processed.	The trust boundary is blurred, since cloud data could span multiple geographic locations.
Complexity of Compliance	Security compliance is limited to the organisation and contracted parties.	The global and dynamic flow of data makes the location of data unpredictable and complicates cloud compliance.
System Complexity	Limited attack surface	Cloud systems are made up of more complex systems, resulting in a larger attack surface.
Internet Dependence	Traditional systems host applications in-house and only rely on the Internet for additional functionality.	Cloud systems are totally reliant on the Internet, and the lack of Internet access leads to loss of productivity.

In summary, this comparison shows that the same way cloud benefits outweigh traditional models, so also does their risks. As data and applications in the cloud are managed outside the trust boundary by a dynamic supply chain, it has become essential for CSPs to demonstrate the implementation of adequate security practices to protect the sensitive data and processes put under their control. Cloud transparency, particularly the visibility of security controls and processes, is likely to become a central theme for improving customer confidence in cloud services and reducing perceived risk.

2.2 Risk Assessment Methodologies

According to the International Standards Organisation (ISO) 27005:2011 standards document, a risk is defined as the effect of uncertainty on objectives [151]. Information security risks lead to a deviation from the expected results for which security controls were implemented, and they impact the objectives of the information asset, including its financial, safety or productivity goals. The concept of risk varies in interpretation and significance

to organisations. Therefore, the risk management and risk assessment approach for each organisation will vary based on their predisposition, in-house expertise and risk appetite.

According to Bojanc [46], the risk management (RM) process typically consists of two main stages, known as risk assessment (RA) and risk treatment (RT). RM is defined as the overall process of managing risk to an acceptable level within an organisation, while RA is the process of identifying, evaluating and prioritising the risks [46]. RM is fundamentally about making decisions about which risk issues are most critical (prioritisation), which risk issues are not worth worrying about (risk acceptance) and how much to spend on the risk issues that need to be dealt with (budgeting) [124]. RA is a central part of information security management and it enables organisations to identify vulnerabilities and threats while also informing the choice of cost-effective countermeasures to address potential threats. Ionita [145] describes RA as a structured or semi-structured approach of analysing the security of a system, identifying weak spots and selecting countermeasures.

RA, and to a more significant extent RM, involves a continuous re-iteration process which revolves around identifying, analysing, prioritising, mitigating and monitoring security risks. Risk assessments are conducted to inform decision-makers and support risk responses, either as part of a security audit, compliance initiative, or to support security budget decisions [145, 258]. While it is impossible to achieve a fully secure system, void of security risks, the overall aim of a security risk assessment is to minimise, monitor and control the probability and impact of disruptive security events. The primary objective behind designing a security risk assessment framework is for security controls to be selected based on real risks to an organisation's assets and operations.

A cross-section of risk assessment methodologies developed by standards and regulatory bodies are as shown in the table 2.4. In section 2.3, we discuss three of these frameworks in more detail, since they were referenced in the development of our proposed cloud model.

2.2.1 Qualitative and Quantitative Risk Assessment

A widely accepted hypothesis is that risk measurement always leads to a trade-off between accuracy and precision. However, a properly executed risk assessment should seek to analyse risks in a way that it yields simple, easy to understand results, capable of being communicated to decision-makers concisely. In this section that follows, we briefly discuss the two main risk assessment approaches.

2.2.1.1 Qualitative Assessment

Qualitative risk assessment employs a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels(e.g., low, moderate, high) [258]. It involves presenting risk assessment results and recommendations in a descriptive form. It is more

Table 2.4: Risk Assessment Frameworks

Risk Framework	Risk Assessment Methodology	Risk Identification	Risk Analysis	Risk Evaluation
Cramm	Qualitative	Yes	Yes	Yes
EBIOS	Qualitative	Yes	Yes	Yes
ISF Methods	Qualitative	Yes	Yes	Yes
ISAMM	Quantitative	Yes	Yes	Yes
ISO/IEC 27005	Qualitative	Yes	Yes	No
IT-Grundschutz	Qualitative	Yes	Yes	Yes
Magerit	Qualitative and Quantitative	Yes	Yes	Yes
Marion	Qualitative	Yes	Yes	Yes
Mehari	Qualitative and Quantitative	Yes	Yes	Yes
MIGRA	Qualitative	Yes	Yes	Yes
Octave	Qualitative	Yes	Yes	Yes
NIST SP800-30	Qualitative	Yes	Yes	Yes
RISK IT (ISACA)	Qualitative	Yes	Yes	No
FAIR	Qualitative and Quantitative	Yes	Yes	Yes

commonly used than the quantitative method and is known to be popular within small and medium-sized companies [53]. According to the ISO/IEC 31000:2009 [152], the qualitative approach is used in events where it is difficult to express a numerical measure of risk, such as, during the initial assessment to recognise risks. Due to its representation of vulnerability level, impact and consequences with descriptive values, Burtescu [53] argues that this can lead to incorrect risk values. In [167], authors identified the subjectivity of qualitative risk assessment as a major drawback. At the same time, the UK research organisation, JISC [158], states that people are not good at analysing risk, considering their decisions tend to sway depending on their emotional response to a situation rather than objectively assessing the risk. Likewise, the research conducted by Hubbard[142] claim that experience has shown that the answers of the experts and managers involved in qualitative assessments were often a function of over-confidence, logical errors and random inconsistencies, leading to wrong decisions.

Although qualitative assessments are known to be a quick and easy approach to risk assessment, employing limited rigour, they do not provide enough quantifiable measurements concerning probabilities and impacts of risks [105]. Also, the comparatively small range of values used in assessment makes relative prioritisation or comparison within the set of reported risks difficult. In addressing the drawbacks identified in the method, the recommendation of JISC [158] is for qualitative risk methods to make use of complementary checks such as the application of Delphi method, where opinions are gathered anonymously then cross-checked with a range of experts. Likewise, Liu [190] suggests that for cloud risk assessments, which is often complicated, involving multiple stakeholders, both qualita-

tive and quantitative analysis should be integrated into a combined approach, to avoid the one-sidedness of evaluation results.

2.2.1.2 Quantitative Assessment

Quantitative risk assessment attempts to assign real numbers to assets, and assigns a dollar value to the impact of a threat on the asset should the risk materialise [267]. Quantitative assessments are known to maintain internal and external consistency with the meanings and proportionality of the values used for risk estimation. Furthermore, its ability to provide probabilistic estimates of risk, time and actual dollar amount or 'bottom line' makes it appealing to non-technical decision-makers [32]. This type of assessment, involving the use of a mathematical model, is best suited for security technology investment evaluation and cost-benefit analysis of alternative risk responses, based on its ability to analyse security risks and evaluate critical assets quantitatively. The benefits of quantitative assessments include rigour, repeatability, and reproducibility of evaluation results, but much of the benefit is dependent on the accuracy of the assigned risk values, and the validity of the statistical models used [97].

Over the years, numerous authors have raised concerns about the accuracy of measurement and reliability of quantitative assessments. In [258], there is a concern about the subjective determination of risk values, while Fito et al. [105] argue that the risk calculations have a strong element of arbitrariness. Likewise in [42], quantitative risk analysis was referred to as the 'arrogance of quantifying the unquantifiable', although Bernstein went further to suggest that this did not exempt mathematical models from being used as a complement to expert intuition. About the statistical reliability and the inadequacy of empirical data, which is a common argument amongst critics of quantitative assessment, the industry research conducted by Hubbard and Seiersen [143] have shown that we have more information than we think we do and we need less information than we think. Nevertheless, many have referred to this argument as the logician's trap, claiming that past data from real-life are untrustworthy since they do not provide us with independent observations that the laws of probability demand [42]. By way of counter-argument, both Freund and Jones [112], and Hubbard and Seiersen [143] illustrated how the process of asking questions about the HR screening, the number of administrators of a system, their length of service, employee morale, etc. can inform the estimate of a malicious insider within the IT team and help the risk analyst defend such estimate.

Lastly, despite the use of quantitative assessment in well-developed industries such as Finance/Insurance, Mining and Aerospace, it is rarely used in information technology, based on the difficulty of measuring risk and the lack of historical data [152]. Since measurements are observations that quantitatively reduce uncertainty (i.e. the goal of risk management),

it seems plausible to conclude that the introduction of some amount of error is unavoidable. Notwithstanding, we believe that the use of controlled experimentation, clearly defined model, peer reviews, and calibration (improving the measurement quality) of the expert judges can also increase the objectivity of quantitative assessments [112, 143].

2.2.2 Risk Modelling

NIST 800-30v1 describes a risk model as a model that defines the risk factors to be assessed and the relationship among the risk factors [258](see Figure 2.3). Also, risk factors are characteristics used in risk models as input to determine the risk level during assessments. Risk factors include vulnerability, impact, threat, likelihood, probability, exposure factors and predisposing condition [53, 258]. Aubert et al. suggest that when an organisation is assessing the risk of a supply chain, examples of additional factors that can play a part in the risk cost include supplier size, competition, and vendor interdependence [26]. In the effective risk management of dynamic systems, such as a cloud environment, there is a need for an in-depth understanding of the individual risk factors, and the examination of how the various risk factors are linked to any undesirable outcomes [26, 112]. According to Verendel [318], some of the properties that make security risks a challenge to understand and model include low stationarity (changing rapidly), dependence (correlated attacks against different systems and components), uncertainty (limited information about consequence, factors cannot be directly observed) and economics (interested agents seeking to achieve goal).

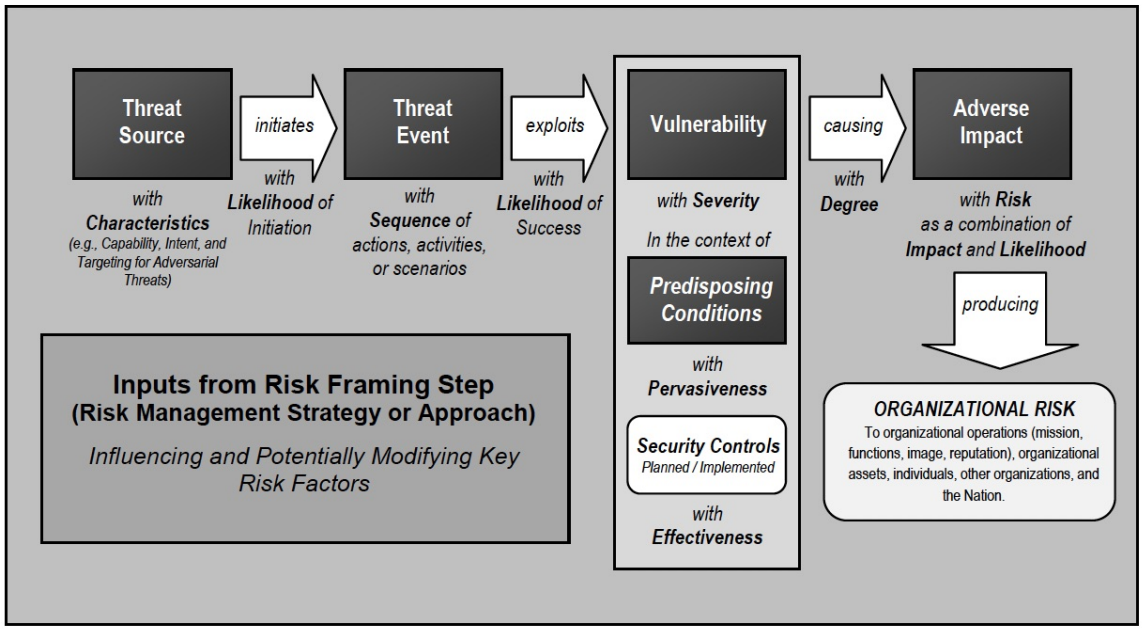


Figure 2.3: Generic Risk Model with Key Risk Factors. This figure has been taken from [258]

The risk management approach for each organisation needs to be unique, and the only way to achieve this is to have a well-founded risk model. Organisations differ on their risk model approach due to a variety of reasons, including their predisposition, in-house expertise, or risk appetite. Both quantitative and qualitative risk assessment methods require the use of a risk model for the analysis of risk. While the quantitative model uses mathematical models such as Monte Carlo and Bayesian networks, most qualitative models are built around mental models of how the human experts think the risk should be assessed, an assumption which sometimes ends up with biased results [112].

Quantitative risk modelling allows risk analysts to analyse each risk scenario, presenting the best and worst-case outcome, with this providing decision-makers a clear picture of their risks. The risk analysis process which involves determining the probability of occurrence of an event, or quantifying the impact of a risk, is often met with a degree of uncertainty which makes it challenging to achieve a consensus [53]. Different members of the risk team are likely to provide different estimations, which is commonly linked to their confidence level or personal perception. This bias in estimation occurs because humans are thought to be poor at estimating "objective risk", and tend to perceive the low probability/high consequence outcomes as riskier than high probability/lower consequence outcomes [79]. Such a challenge can be solved using a mathematical simulation tool such as the Monte Carlo. Other risk models used in cloud security risk assessment methods and tools include the Attack-Defense Trees (ADT), Decision Tree Analysis (DTA), Risk Breakdown Structure (RBS), and Hierarchical assessment indicator system, to name a few [22].

As earlier mentioned, Ross et al. [258] maintains that the risk assessment methodology should include an explicit risk model together with an assessment and analysis approach. Likewise, a risk model can be inductive or deductive [112]. The inductive risk model approach makes use of lots of data to infer the factors of risk and their probability of existence; the approach adopted within the Insurance industry. The deductive risk model is more of an investigative approach and is used when there is limited data, as often experienced in assessing information security risk. The deductive model infers risk elements and their relationship based on experts experience, logic, and critical thinking [112]. It is worth mentioning that a large chunk of the time spent conducting a comprehensive risk assessment is often spent deciding on the risk model, identifying the risk and risk factors and scoping the risk exercise. Time dedicated to risk modelling is not wasted, particularly as touching quantitative risk assessment, because the risk estimate for each risk scenario is reusable for the duration of the system.

In conclusion, while the risk models built for cyber risks are nowhere as complex as the systems being modelled, there is a need for us to re-consider our outlook to risk factors such as threat and vulnerability [143]. The Open Group describes a threat as the capacity

of an actor to cause a loss event to occur, while vulnerability is referred to as a gap in control that increases the chance of a loss event [124]. This definition implies that both threat and vulnerability can be considered as a value instead of a thing. Bearing this in mind, it becomes easier to think of risk as a mathematical product of the probable frequency and probable magnitude of a future loss [112, 124, 143, 172]. We agree with this approach because as earlier established, risk analysis is based on imperfect data and models. Therefore, the expression of frequency or magnitude should contain elements of that uncertainty, especially in a probabilistic form.

2.3 Frameworks Referenced in our Proposed Model

Despite the limitations of traditional risk assessment frameworks in assessing cloud risks, they act as a good foundation for the design and development of conceptual models targeted at the problem area. In this section, we describe three of the existing risk assessment standards and guidance documents, i.e. ISO/IEC 27005:2011, NIST 800-30v1 and Factor Analysis of Information Risks (FAIR) methodology, which have been referenced in the development of the proposed model presented in this thesis.

2.3.1 NIST SP 800-30 rev1

NIST developed the Special Publication (SP) 800-30v1 [258]. The purpose of the document is to provide federal information systems and organisations with guidance for conducting risk assessments, amplifying the guidance in NIST SP 800-39 [257]. Being a guidance document, the SP 800-30 rev1 offers organisations maximum flexibility on how risk assessments (RA) are conducted, without placing any specific requirements on the formality, rigour, method, tools, or format of risk assessment results. However, NIST advises that because of the ongoing nature of risk management, risk assessments are to be conducted throughout the system development lifecycle. The guidance supports the organisation in addressing their RA needs, including integrating risk assessment into their broader risk management processes. Furthermore, the guidance supports transparency by encouraging organisations to share risk-related information.

According to NIST [258], risk assessment is defined as the process of identifying, estimating and prioritising information security risks, while risk is expressed as a function of the likelihood of a threat event's occurrence and the potential adverse impact, should the event occur. Highlighting the purpose of an RA, NIST 800-30 identifies how RA informs decision-makers and support risk responses by identifying:

- The relevant threats to the organisation or through the organisation to other organisations;

- Organisation's internal and external vulnerabilities;
- Impact to organisations due to the potential for threats to exploit vulnerabilities; and
- Likelihood that harm will occur.

The risk assessment method adopted by the NIST 800-30 includes:

1. A risk assessment process
2. An explicit risk model
3. An assessment approach
4. An analysis approach

The guidance document states that organisations can increase the reproducibility and repeatability of risk assessments by making explicit the risk model, the assessment approach, the analysis method and the rationale for estimating risk factors. We will now briefly describe each of the steps, starting with the risk model.

1. Risk model - A risk model defines the risk factors to be assessed and the relationships among those factors [258]. Five (5) risk factors are identified in the NIST 800-30 document, and they are:
    - *A threat-* is any circumstance or event with the potential to adversely impact organisational operations and assets, individuals, organisations or nation through an information system.
    - *A vulnerability-* is any weakness in an information system, system security procedure, internal controls, or implementation that can be exploited by a threat source.
    - *A predisposing condition-* is a condition that exists within an organisation, information system, or environment of operation, which affects the likelihood that threat events, once initiated, will result in adverse impact for the organisation or its assets.
    - *The likelihood of occurrence-* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).
    - *The level of Impact-* is the magnitude of harm that can be expected to result from the consequences of unauthorised disclosure, modification, or destruction of information, or the loss of information or information system availability.

2. Assessment Approach- Three approaches are discussed in NIST 800-30 rev1 for assessing risk and its contributing factors, each having their advantages and disadvantages: Quantitative, Qualitative and Semi-quantitative.

    - *Quantitative Risk Assessment*- typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers.
    - *Qualitative Risk Assessment*- typically employ a set of methods, principles, or rules-based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high).
    - *Semi-quantitative Risk Assessment*- typically employ a set of methods, principles, or rules that uses bins, scales, or representative numbers whose values and meanings are not generally maintained in other contexts (e.g., 0-15, 16-35, 36-70, 71-85, 86-100).

3. Analysis Approach- The analysis approach differ with respect to the orientation or starting point of the risk assessment, its level of detail and how risks due to similar threat scenarios are treated. The three analysis approach discussed in the 800-30 rev1 are as follows:

    - Threat-oriented
    - Asset/Impact-oriented
    - Vulnerability-oriented

4. The Risk Assessment process-, The process of conducting a risk assessment using the NIST SP 800-30 rev1 guidance, is composed of four steps. Each step is divided into a set of tasks, as shown in Figure 2.4. The RA process makes it possible for ongoing communication and information sharing to take place among stakeholders, to ensure that the inputs are as accurate as possible and that the intermediate RA results can be used for assessing other direct or indirect stakeholders. Also, the RA process enables organisations to use the result of an assessment as useful input for the risk response or treatment aspect of the risk management process.

2.3.2 ISO/IEC 27005:2011

The ISO/IEC 27005 [151] provides organisations with risk management guidelines and does not enforce a specific method, thereby, leaving it to organisations to define their approach based on scope, their context of risk management, or industry. Although the ISO/IEC 27005 can be applied as a standalone document, some knowledge of the concepts, models,

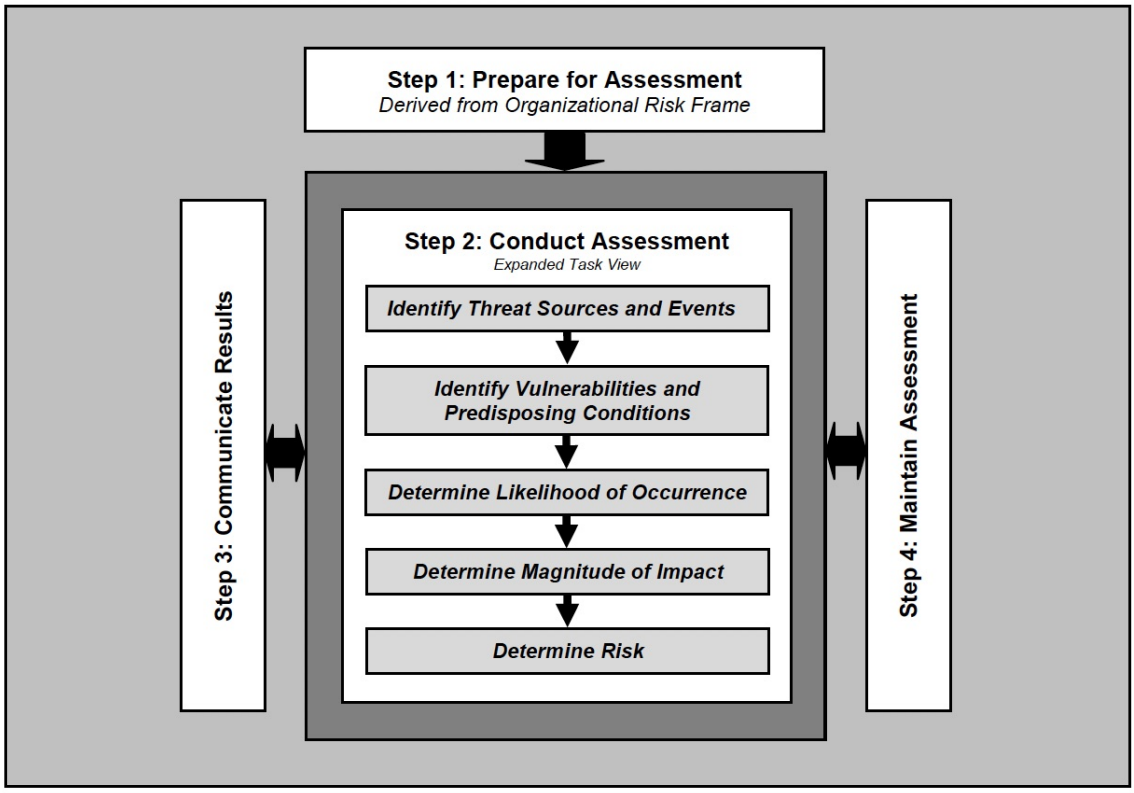


Figure 2.4: NIST SP 800-30 Risk Assessment process. This figure has been taken from [258]

processes and terminologies described in ISO/IEC 27001 & 27002, are important for a complete understanding of this standard. The standard supports a systematic and continuous approach to information security risk management, beginning with establishing an external and internal context, assessing risks, treating the risks and promoting decision-making. Seeing that we are only interested in the risk assessment element of the standard, we will now describe the processes that lead up to assessing risk under the ISO/IEC 27005 standard (i.e. Clause 6, 7 & 8).

According to the ISO/IEC 27005 standard, the information security risk assessment should assist organisations with identifying risk, assess risk based on their consequences to the business and the likelihood of their occurrence, communicate risk and assess the effectiveness of security controls [151]. Figure 2.5 shows the iterative approach ISO/IEC 27005 takes in conducting a risk assessment, where the depth and detail included in the assessment can be increased with each iteration. Considering that the effectiveness of the risk treatment depends on the results of the risk assessment [151], the RA process is tasked with providing sufficient information needed to modify risks to an acceptable level, else the iterative process continues.

Before commencing a risk assessment exercise, the organisation should already have in place, an internal and external context for their information security risk management. Con-

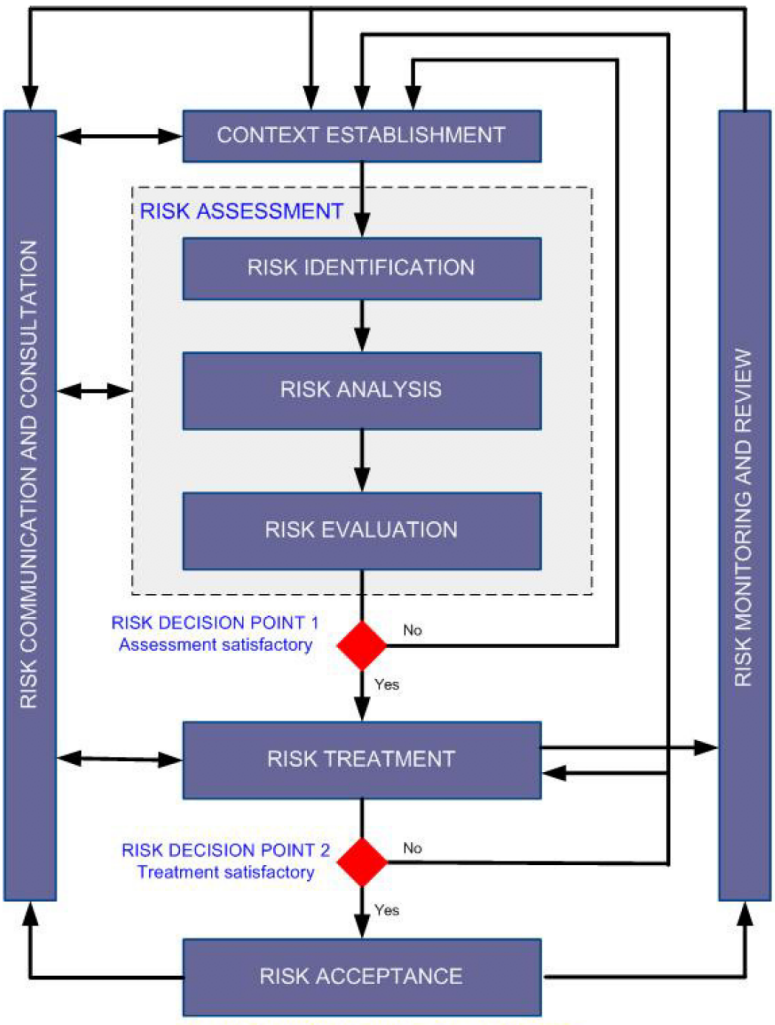


Figure 2.5: ISO/IEC 27005:2011 Risk Management process. This figure has been taken from [151]

text establishment addresses basic criteria such as risk evaluation criteria, impact criteria and risk acceptance criteria [151]. The risk evaluation criteria evaluate the organisation's information security risk based on the following:

1. Strategic value of the business information process;
2. Criticality of information asset;
3. Legal & regulatory requirements;
4. Operation and business importance of availability, confidentiality and integrity;
5. Stakeholder expectations and consequences for goodwill and reputation.

Likewise, the impact criteria specify how the degree of damage or cost to the organisation is expressed following a security event. Furthermore, the organisation defines their risk

acceptance criteria, which often depends on their policies, goals, objectives and stakeholder interests. Lastly, the pre-work activities for the risk assessment include defining scope and boundaries, to ensure that all relevant assets are taken into account in the risk assessment [151].

The ISO/IEC 27005 standard defines risk as a combination of the consequences of an unwanted event and the likelihood of the occurrence of the event [151]. It states that the purpose of risk assessment is to quantify or qualitatively describe the risk to enable managers to prioritise risks according to their perceived seriousness or established criteria. The risk assessment process consists of the following activities:

1. Risk Identification - The risk identification process helps to gain insight into how, where and why an event can cause a potential loss. According to the standard, risk identification should aim to include risks even when the risk source is not under the control of the organisation (supply chain). Some of the activities that take place during this stage include the identification of assets, threats, existing controls, vulnerabilities and consequences.

2. Risk Analysis - The degree of detail involved in the conduct of risk analysis depends on the criticality of assets, the extent of vulnerabilities known and prior incidents in the organisation. The risk analysis methodologies supported under the ISO/IEC 27005 standard include the quantitative, qualitative, or a combination of both[151]. Other activities include the assessment of consequences, assessment of the incident likelihood and the level of risk determination.

3. Risk Evaluation - The risk evaluation is the third and final stage of the risk assessment process. During this stage, a list of risks has been identified, together with value levels assigned and what is left is for decisions to be made based on the risk evaluation criteria. In evaluating risks, organisations compare the estimated risks with the evaluation criteria defined during the context establishment stage. The risk evaluation also takes into consideration the objectives of the organisation, stakeholder views and the degree of confidence in the risk identification and analysis stage. Risk evaluation uses the understanding of risk to make decisions about the future based on the acceptable level of risk.

2.3.3 FAIR

FAIR (Factor Analysis of Information Risk) is a taxonomy of the factors that contribute to risk and the interaction between these factors. It was developed by Jack Jones [162] and was later adopted as a standard by the Open Group [112, 124]. FAIR provides a framework for understanding, analysing and measuring risk by decomposing information

risk into its fundamental parts [112]. The FAIR approach is primarily concerned with establishing accurate probabilities for the frequency and magnitude of loss events [112, 162]. The strength of the FAIR method lies in how it complements the works of other standards bodies, e.g. OCTAVE, NIST 800-30, ISO/IEC 27002:2005 [124]. Based on its advanced analysis, the FAIR framework aims to establish consistent, defensible statements about the value of risk. It cautions against making unnecessary assumptions in risk analysis, especially with the critical aspects of the risk environment. The FAIR method emphasises the value component of information risk and describes risk as a combination of threat event frequency, vulnerability, asset value and liability characteristics.

FAIR defines risk as the probable frequency and probable magnitude of future loss [162]. It maintains that risk is a probability issue since the probability reflects the continuum between absolute certainty and impossibility. Although FAIR admits that there are no credible information security risk data, a situation it credits to the inability of the Information system industry to normalise against a standard taxonomy, it points out that non-data driven analyses have been successfully adopted in other industries, such as medical diagnosis, missile targeting, marketing and investment [162].

The FAIR framework identifies four primary risk landscape components : *threats, assets, the organisation and the external environment.* A taxonomy of the factors that make up information risk under FAIR is depicted in Figure 2.6 and defined as follows [162, 112, 124]:

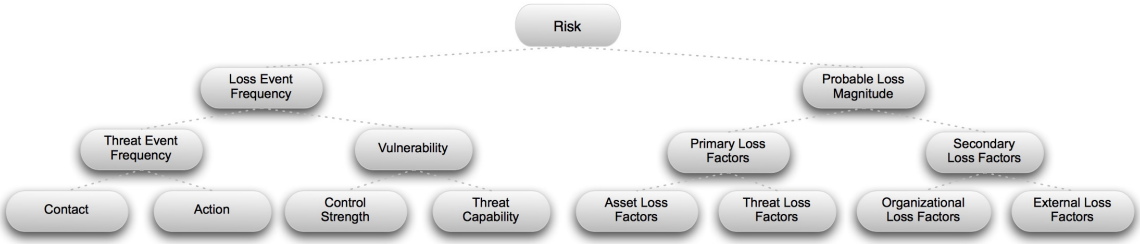


Figure 2.6: Decomposition of Risk according to the FAIR framework. This figure has been taken from [162]

1. **Loss Event Frequency (LEF)**- is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset. This factor is decomposed into two other factors: Threat Event Frequency (TEF) & Vulnerability.

2. **Probable Loss Magnitude (PLM)**-Estimating loss is one of the difficult aspects of analysing risk, particularly due to the lack of precision on asset value, the different forms of loss and the complex systemic relationship between the different forms of loss. Forms of loss include productivity, response, replacement, fines and judgement, competitive advantage and reputation. FAIR divides PLM into two groups: Primary & Secondary Loss Factors.

Other concepts introduced in the FAIR framework include:

- *Threat Communities* - subset of the overall threat agent population that share key characteristics.
- *Threat* - is anything (e.g., object, substance and human) that is capable of acting against an asset in a manner that can result in harm.
- *Asset* - any data, device, or other components of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, or stolen, resulting in a loss.
- Controls - All controls can be characterised through three dimensions. They are Forms (policy, process, or technology), Purpose (preventive, detective, or responsive) and Categories (loss event, threat event and vulnerability).

FAIR presents a flexible methodology for risk assessment to ensure that practitioners can tailor it to meet the needs of the decision-makers. The Core Unified Risk Framework (CURF) for estimating the completeness of risk assessment methods, evaluated the FAIR method as one of the most comprehensive frameworks for conducting risk estimations [324]. Acknowledging the subjectivity inherent in human judgement, one of the goals of FAIR is to bring as much objectivity into the risk analysis process as possible. FAIR supports the use of either qualitative or quantitative methods but emphasises that the decision to use either measure should be driven by the needs of the decision-makers and credibility of the available methods [162].

In conclusion, the basic FAIR analysis is comprised of ten steps divided into four stages [162]:

1. **Stage 1 - Identify scenario components**
   - Identify the asset at risk
   - Identify the threat community under consideration
2. **Stage 2 - Evaluate Loss Event Frequency (LEF)**
   - Estimate the probable Threat Event Frequency (TEF)
   - Estimate the Threat Capability (TCap)
   - Estimate Control strength (CS)
   - Derive Vulnerability (Vuln)
   - Derive Loss Event Frequency (LEF)

3. **Stage 3 - Evaluate Probable Loss Magnitude (PLM)**

   - Estimate worst-case loss

   - Estimate probable loss

4. **Stage 4 - Derive and articulate Risk**

   - Derive and articulate Risk

2.3.4 Summary

One of the main conclusions that can be drawn from this review is that while the majority of RA Standards and guidance documents have many things in common, there are noticeable variations in their approach, scope and applicability. Due to the broad applicability of most of the popular RA/RM frameworks, e.g. ISO/IEC 27005, ISO/IEC 31000 and NIST 800-30v1, they describe risk assessment at an abstract level and do not offer sufficient practical guidelines for completing each step. Also, being predominantly qualitative or semi-quantitative, the use of these traditional risk frameworks in assessing cloud risks is often judged as limiting in scope. Based on the three RA methods reviewed, the FAIR method is considered to be the most complete security risk assessment model. FAIR complements the older standards and looks to improve the objectivity of risk results by considering more risk factors, adopting a probabilistic approach and decomposing risks into its fundamental parts. According to Albakri et al. [19], most common risk assessment standards assume that an organisation's assets are managed in-house and that security management processes are compliant with the organisation's standards. Therefore, applying such risk assessment frameworks to the cloud leads to increased vulnerabilities and inadequate implementation of security controls.

Overall, we maintain that the process of manually fitting the traditional risk assessment frameworks to address cloud risks is unsuitable for the dynamic environment. Therefore, a more practical approach will be for new cloud risk frameworks to be built from the ground up to address the various shortcomings of the current risk models.

2.4 Cloud Supply Chain

According to New & Westbrook, a supply chain is more than a metaphor [217]. They define a supply chain as a series of links between suppliers and their customers until a product or service reaches its ultimate end-user [217]. Wisner et al. [330], also defines a supply chain as the series of companies that make products and services available to consumers, including all the functions enabling the production, delivery and recycling of materials, components, end products and services. There is a relatively small body of literature that goes into any length to address the supply chain or value chain of cloud services [45, 247].

Notwithstanding, we define cloud supply chain as a network of key actors that work together to provide, develop, host, manage, monitor or use cloud services; each facing internal and external risk factors and influences that make it uncertain whether and when they will achieve their cloud service objectives. The supply chain is the core of every cloud service delivery, and it consists of globally-distributed and dynamic collections of people, processes and technologies that encompass various software and hardware components [61].

The term 'cloud supply chain' was coined out of more traditional terms such as IT supply chain and cyber supply chain to represent the processes, products, data and participants involved in the delivery of a cloud service. Besides, Boyson et al. [50], define cyber supply chain as 'the entire set of key actors involved with/using cyber infrastructure: system end-users, policy-makers, acquisition specialists, system integrators, network providers and software/hardware suppliers. Lindner et al. reckon the application of supply chain concept to cloud computing to be innovative and suggests the possibility of a new research field [188]. We identified five essential elements involved in the delivery of a cloud service and present it using Figure 2.7.

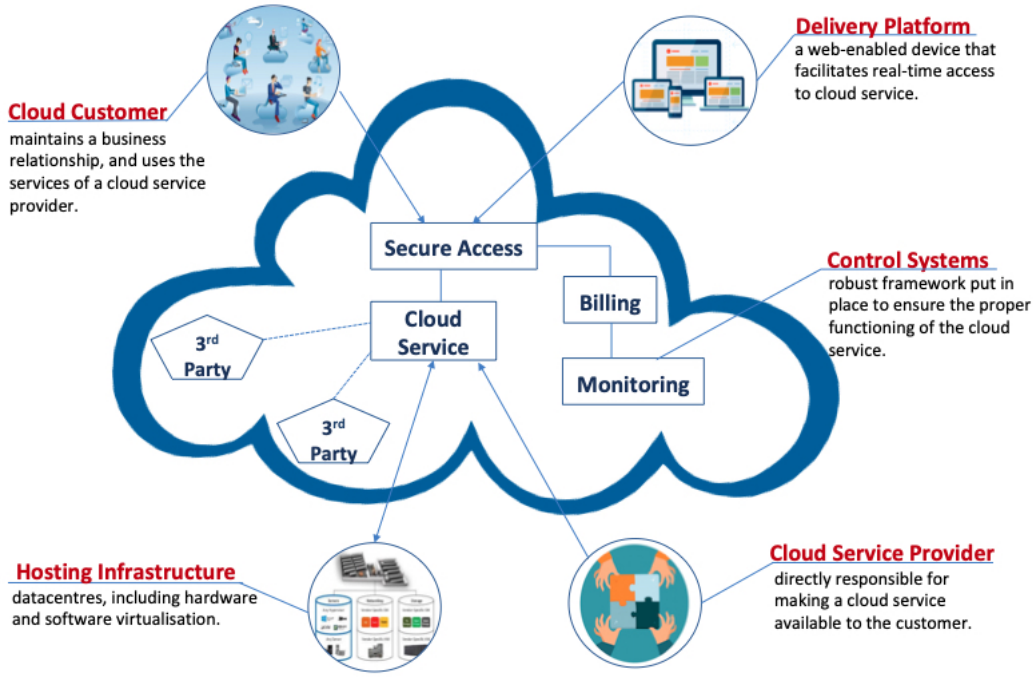


Figure 2.7: The essential elements of a Cloud Service

The cloud supply chain is an end-to-end process, which is not limited to the delivery of services but includes other aspects such as market mediation, security, billing, legal, performance monitoring and accountability [188, 237, 326]. All actors within the cloud supply chain, exchange services for money, and add value to other actors' offering through the refinement of services that ultimately fulfil customer needs [183]. However, organisations that use or provide cloud services operate in a complex and dynamic environment, involving

multiple supply chains and these CSPs need to feel confident that suppliers further down that chain are accountable for how they manage personal and confidential data [101]. Cloud migration or the setup of cloud infrastructure does not eliminate the management of traditional IT assets, which increases the complexity of IT operations. The complexity resulting from the large-scale virtualisation and data distribution in the cloud has been known to drive the call for better cloud accountability and shifting customer security concerns from server to data [174]. Also, there is a core issue of heterogeneity, where CSPs and customers are unable to determine if suppliers comply with platform and development standards accurately. With the "API Economy" dictating the speed of cloud innovation and development teams working on aggressive sprints, the security properties of many best-of-breed cloud solutions cannot be guaranteed.

Also, due to the dynamism of the cloud supply chain, it is believed to be less predictable and highly volatile, particularly when compared to traditional IT, which is based on a relatively fixed supply chain network [188]. Cloud services are exposed to dependency risks which can be due to supplier platform migration, net-new development done in a silo, or a failure of an indirect third-party. Nonetheless, some of these cloud concerns can be neutralised by the design of a resilient architecture [84, 281] and the simplification of cloud development and management processes. While Abbadi and Lyle identified the advantages of the dynamic nature of the cloud, such as flexibility and scalability, they also acknowledge its introduction of new security, logging and auditing challenge [1]. Similarly, Pearson argues that a dynamic supply chain enables businesses to strike a balance between the opportunities that drive economic growth and the downside risks of disruptive events that might occur from the failure of a member of the chain [243].

2.4.1 Cloud Supply Chain Risks

Quantifying security risks in supply chains has become a central challenge in risk management [30]. Boyens et al. [48] demonstrate how managing ICT supply chain risks could be a complex, multifaceted undertaking that requires a coordinated effort across an organisation. Cyber supply chain risk management (CSCRM) is a new discipline designed to address the challenges of rapid globalisation and outsourced diffusion of hardware and software systems [49]. Considering this is a nascent area of research, there is no widely accepted definition for cloud supply chain risk. So, in simple terms, we define cloud supply chain risk as the probability of an internal or external event targeted at a cloud service or its extended network of suppliers, causing a disruption or failure to cloud operation and leading to reductions in service levels and security posture.

Cloud risks are associated with the processes, procedures and practices used to assure the integrity, security, resilience and quality of cloud services [48]. These risks (per-

ceived/actual) are further exacerbated by the high rate of technological change and the dynamically complex supply chain network. In [159], Johnson categorised supply chain risks into two categories: direct and indirect supply chain risks, where the direct risks affect the focal CSP providing the cloud service, and indirect risk threatens the computational infrastructures that support sub-contractors.

Our reflection on literature identified a significant number of reports addressing the existence of supply chain security risks in cloud computing, but only a few recommended solutions to these risks [194, 209]. According to Jenks [157], there is a gap between the 'what' and 'how' processes of managing cloud supply chain cybersecurity risk. This view is supported by the Federation of Small Business (FSB), who in a recent study found that about 65% of UK SMBs do not have plans in place to deal with potential supply chain disruption [225].

Moreover, the cloud supply chain employs "aggressive sourcing" based on free-market principles rather than collaboration, which increases cloud risks. Risks associated with the processes, procedures and practices used to assure the integrity, security, resilience and quality of cloud services increases with the on-demand, automated and multi-tenanted cloud, down the supply chain [48]. Cloud services are exposed to new threats capable of exploiting the technology, process and organisational vulnerabilities associated with cloud service delivery. Boyens et al. [48] aptly observe that cloud supply chain risks are associated with an organisation's decreased visibility into and understanding of, how the technology that they acquire is developed, integrated and deployed. Wisner et al. [330] however reckon that the best way to manage supply chain risk is to increase supply chain visibility.

2.4.2 Transparency, Trust and Risk Assessment

Numerous scholars have written extensively about the in-depth connection between transparency and trust [70, 90]. Other research works have also considered the effect of transparency on risk [61, 216]. However, only a few of these studies have addressed issues in the technology sector, particularly cloud computing. According to industry reports by Pearson [241] and Schneier [275], the low level of consumer trust resulting from the lack of cloud provider transparency has resulted in new and unquantifiable security risks. Also, Albert S. & Rajeev [181] hold the view that improved visibility of the supply chain helps customers to determine the trustworthiness of a cloud service a priori, based on its profile and security assurances.

According to the Business Dictionary [87], transparency is the minimum degree of disclosure to which agreements, dealings, practices and transactions are open to all for verification. Sigler et al. [286] also define transparency as the full understanding of the execution and outcomes of a process among a defined set of stakeholders or partners. Cloud security

transparency is defined in [150] as the disclosure of security-related practices and controls used for the protection of customer data and applications hosted in the cloud environment. CSP transparency is an essential means for strengthening information disclosure, and it enhances users' trust in cloud services.

Werff et al. [327] defined trust as a three-stage process consisting of positive expectation, the decision to make oneself vulnerable to another party and a risk-taking act. In [264], the author makes a distinction between contractual, competence and goodwill trust. Also, in the work of Sung & Kang [300], the authors list long-term & repeated interaction, information sharing & reciprocity and interdependence & asset specificity as the determinants of trust level between firms. In cloud supply chains, trust is one of the fundamental cooperation factors [125].

To establish the interconnectedness between transparency, trust and risk assessment, Kaliski-Jr and Pauley [165] point out that an increased level of trust improves disclosure and reduces perceived risk, while Pearson [241] concludes that risk assessments provide significant value in increasing trust in commercial services. In Figure 2.8, we show how each element contributes to improving consumer perception of cloud adoption risks.

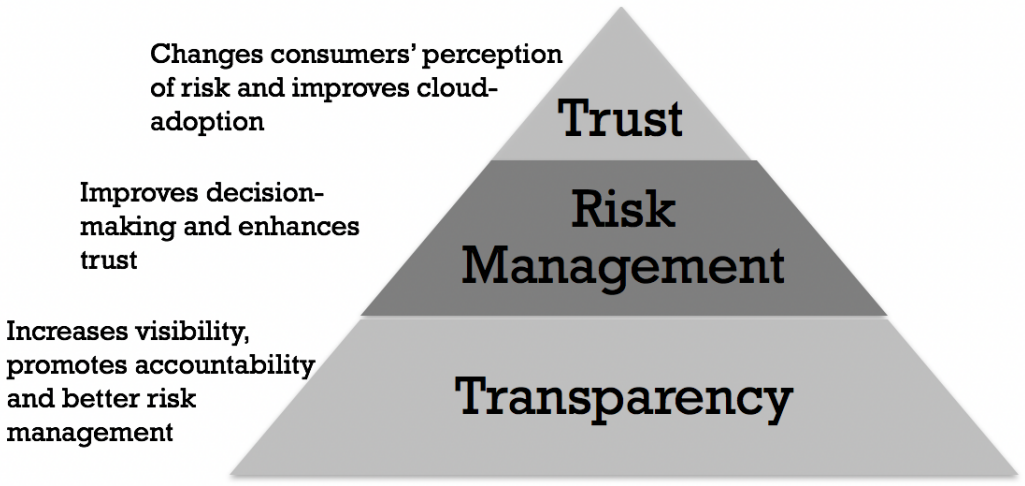


Figure 2.8: Transparency, Trust and Risk Management between CSP and CSC

As stated by the Centre for the Protection of National Infrastructure (CPNI), the awareness or visibility of third-party risks is the key to effective risk management [72]. Likewise, the ISO21000 highlights transparency and inclusivity as part of the principles for a successful risk management [317]. ENISA reckons that the primary challenge with assessing the risk of cloud computing stems from the fact that the data that is needed to estimate the impact and likelihood of risk scenarios or events are either unavailable or inadequate [97]. Likewise, Power [245] suggests that this level of transparency is hindered by reputational

risk, which many organisations are worried about, especially firms in charge of managing risks on behalf of their customers. New [215], supports this argument from a liability standpoint, stating that organisations become more liable the more they know about their supply chain. An example of this lack of transparency in the cloud industry is found in CSA's report on cloud outages between 2008 and 2013. The report listed 172 unique cloud incidents, but only 129 (75%) providers declared the cause of the outage, while 43 (25%) failed to attribute their outage to a particular vector [173].

That said, the CSA and ISACA organisations in promoting cloud security transparency, connect the elements by saying that: "the transparency into the adequacy of the system of internal controls provides trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk" [148].

2.5 Systems Thinking

The world today is experiencing accelerated growth in the number of complex systems that play crucial roles in the social and economic space. The newly developed technologies have an increasing interdependence on pre-existing systems (e.g. cloud and edge computing dependent on the Internet) and produce extremely complex and unpredictable effects. Herbert Simon [288] defined a complex system as one made up of a large number of interacting parts, where the whole is more than the sum of the parts in a practical sense. A cloud service (e.g. CRM application) is an example of a complex system. The supply chain of a cloud service is made up of many agents (providers, users, components), all of which interact in intricate ways leading to a continual reshaping of the service and its delivery [27]. An agent is an individual "actor" in a complex environment [27].

Before going any further, we make a distinction between complex, complicated and chaotic systems. Complex systems differ from chaotic ones, in that chaos deals with situations where systems are sensitive to small changes, and rapidly become disorderly and unmanageable. Although, despite appearing to have a random appearance, chaotic systems have some underlying order to them [315]. Complexity deals with systems composed of many interacting agents, who interact in a non-linear way, thereby affecting the probability of later events. Complex systems feature feedback loops and exhibit emergent behaviours [115]. By emergent, we mean properties which are not noticed in isolation but result from the interactions and dependencies between the system components [119]. This provides insights into the robustness of the underlying system [205]. Complicated systems, however, are understood by the sum of their parts. They are complicated because of a large number of parts, not because of the nature of interactions between those parts [115].

Cloud services can also be classified as a complex adaptive system, seeing that the agents involved in the system are capable of evolving and are actively trying to improve

themselves (i.e. adapt). Cloud computing is made up of a dynamic network of interacting components, involved in information exchange, and their relationship is not an aggregation of the individual static entities [64]. As a complex system, the perfect understanding of the individual components of a cloud service does not automatically convey a perfect understanding of its behaviour [205]. The interactions that take place within a cloud supply chain are non-linear, seeing that a small change along the chain could have a significant effect on the cloud system. Cloud services run in distributed environments, where there are many moving parts, which can fail any time [168]. Nowadays, information systems are highly dynamic and are characterised by constant technological change. Developing cloud applications which rely on external components to function, requires that the potential risk scenarios be modelled into the development, and mitigation mechanisms be put in place to recover from such failure.

Modelling for risk scenarios in complex systems requires a systems thinking approach, where each entity involved in the delivery of the service is identified, and the relationships and dependencies between the entities are mapped out. Systems thinking enables us to make explicit models to look at the combination of the interdependent component systems that make up a cloud service and study how the state of the cloud system changes as a result of the interactions of these components [3]. This broad approach to understanding how complex systems fit together, originated from Ludwig von Bertalanffy's work on General systems theory during the 1950s [322]. General systems theory was targeted at understanding "wholeness", and it is based on the principle of the whole being more than the sum of its parts. Complex systems is a subset of systems theory, although General systems theory studies a much broader class of systems including non-complex systems, where traditional reductionist approaches may remain viable. Systems thinking like the General systems theory attempts to elucidate deep principles underlying systems whose components are linked by feedback loops [244]. Its approach seeks to understand how system components interact and how the underlying systemic relationships and dependencies impact behaviour, both of which help to expand knowledge about the system as a whole.

The academic literature on systems thinking has revealed the emergence of several contrasting themes. The theories embedded in systems thinking have at least a 60+ year history, starting with Ludwig von Bertalanffy's work on wholeness [107, 322]. Also, Herbert Simon [288] in his paper titled "the architecture of complexity", attempted to describe the composition of complex systems. He showed that complex systems were composed of sub-systems that were hierarchically organised, describing how the near-decomposability property of hierarchies simplified the behaviour of these complex systems [288]. Systems thinking expresses our understanding of dynamic complexity [301], and it makes use of tools such as causal loop diagrams, stock and flow diagrams, simulation models to show the

relationship between entities instead of studying them in isolation [71, 217]. It focuses on interaction, entailment, dependencies, exchange, connections and relationships [71]. Arnold & Wade [24] after considering previous definitions of systems thinking, defined systems thinking as a set of synergistic analytic skills used to improve the capability of identifying and understanding systems, predicting possible behaviours and devising modifications to them in order to produce desired effects. This aligns with our use of the approach in this thesis, seeing that the interdependency of cloud components demands systems thinking [63, 108].

Systems thinking could be described as interdisciplinary. It is grounded in the theory of non-linear dynamics and feedback control developed in engineering, physics and mathematics disciplines, but also draws on cognitive and social psychology, organisation theory and other social sciences [107, 297]. Systems thinking helps to see both the forest (i.e. system) and the trees (i.e. components), with the system being more than just a collection of its parts. With the traditional problem-solving (reductionist) approach no longer sufficient in addressing complex systems, the systems thinking approach offers a more generalist approach to problem-solving [298]. Using available data, stakeholders can visually represent complex systems to reflect the conceptualisation of reality [312]. This acts as a memory aid, seeing that stakeholders can offload cognition to an external artefact, where it can be analysed. The approach also helps stakeholders to recognise their limitations and correct their cognitive biases about the system (in our case, cloud service).

Systems thinking gives us the ability to think abstractly in order to [24, 295]:

- Incorporate multiple perspectives;
- work within a space where the boundary or scope of the problem may be fuzzy;
- Understand diverse operational contexts of the system;
- Identify component relationships and dependencies, and
- Understand complex system behaviour

While it is still challenging to predict the behaviour of complex systems, the systems thinking approach provides us with thinking skills that are effective in answering questions such as "what to include" in assessment or to think about the big picture (10,000 meters). It assists modellers to reduce a complex description of a system to a simpler one by abstracting out what is unnecessary to include only elements whose interaction are capable of self-generating the intended effect in the model [287].

The modelling of complex systems also calls for a broad boundary, where there are few exogenous variables. The boundary encloses the system of interest [110]. However, like most

open systems, it may be challenging to define system boundaries accurately. Cloud system boundaries due to the nature of interactions between cloud components within a system and between the system and its environment, can be highly dynamic in comparison to traditional IT, which maintains control of almost all aspects of their applications. Therefore, seeing that systems thinking is not a purely technical solution, Sweeney & Sterman has encouraged systems thinking modeller to be prepared to carry out activities ranging from understanding system interaction, identifying non-linearities, and recognising and challenging boundaries of existing mental and formal models [301]. Axelrod and Cohen [27] reckon that by so doing, we will be able to use our knowledge of the system's complexity to improve its performance, or in our case, assess its risk.

2.6 Decision Support Analysis

Decision analysis cuts across multiple industries and is an essential element of risk assessment and mitigation [186]. Risk management is primarily about making better decisions. The risk analysis process is inherently about forecasting the future of a system based on identified risk factors and providing the information to decision-makers. An essential aspect of decision making is to formulate the decision problem into a formal and rigorous form [252]. The organisation's requirements in areas such as security, functionality, performance and usability, often influence the decision involving the selection of a cloud provider.

Decision support models have played various roles over the years, including; i) aiding decision-makers, ii) bootstrapping decision-makers by replacing them with their representations, and iii) as a contrast to decision-makers such as in clinical vs statistical controversy [82]. Human judges are sometimes referred to as imperfect mediators between input and output. They are known to introduce unreliability by their inconsistency and invalidity to the degree that their judgement, which is often based on selected anecdotes, negatively impact the ability of these predictive models. The research of Dawes and Corrigan [82] shows with examples, how random linear models such as Dawes model, yields predictions that are superior to those of human judges. The research of Dawes et al. [80] considered the judgemental accuracy of consultants, based on two approaches to decision-making, i.e. clinical (subjective) and actuarial (statistical) methods and found the actuarial process to be superior.

Seeing that the goal of decision support analysis is not limited to improving the accuracy of human experts, but to improving the transparency, consistency, adaptability and speed of decisions, its use within the cloud industry has been limited to less formal approaches. Examples of studies conducted to bridge this gap include the work of Cayirci et al. [58] who developed the Cloud Adoption Risk Assessment Model (CARAM), a multi-criteria decision approach with the posterior articulation of cloud customer preferences for relative

risk analysis. Likewise, the research of Liu [190] adopted the theory of analytic hierarchy process (AHP) and correlation coefficient to analyse multiple objective decisions as part of their new risk assessment model for information systems in the cloud. Another approach to decision analysis during cloud computing risk assessment is the use of fuzzy logic, as exemplified in [278]. Furthermore, the works of Zoie et al. [338], builds on the Service Measurement Index (SMI) [285], to develop the hybrid DANP framework, a combination of Decision-Making Trial and Evaluation Laboratory (DEMATEL) method and Analytical Network Process (ANP), for cloud decision making.

Taking a structured and disciplined approach to improving the objectivity of decision analysis within the cloud industry, therefore, requires that input is gathered from different stakeholders (business, technical and security) as part of the multi-criteria decision making (MCDM) process. This approach is a move away from intuitive decisions, and such arrangement enables the systematic use of available information to arrive at the possible outcomes, which helps with decision making despite the uncertainties. Studies have shown that the use of models such as the Dawes: based on the Z-score method of unit-weighted regression [81]; the Lens model of Brunswik [51]: based on the use of multivariate regression; or the Bayes model: based on the Bayes Probability [37], can be applied to the decision-making process of the cloud. However, notwithstanding the immense potential of each of the models at conceptualising the human decision process, we are leaning towards the Dawes model based on its simplicity and the empirical evidence from published works that suggests that the method marginally outperforms unaided decision-makers [81, 142]. Ultimately, we aim to have a decision analysis solution that is adaptable, portable, cost-efficient, understandable and traceable.

2.6.1 Z-Score

A Z-score (Z_i) is a statistical measurement of a score's relationship to the mean in a set of scores. It measures how many standard deviations a score is above or below the population mean [140]. The Z-score was initially known as the Altman Z-score, named after Edward Altman, who developed and introduced the formula in 1968 [21, 144]. At its inception, the Z-score was applied to the time-consuming and somewhat confusing process of predicting the financial health of a firm and its closeness to bankruptcy. Variants of the Z-score model are also used as a proxy for bankruptcy risk in areas such as merger and divestment, asset pricing and market efficiency, capital structure determination, pricing of credit risk, distressed security and bond ratings [6]. The use of Z-score models has also been extended to the medical profession, as shown in [95]. Here, Ellis et al. conducted a study to develop an anthropometry-based prediction model for the assessment of bone mineral content in children, correctly predicting bone mineral deficits in children with diseases such as cystic

fibrosis. Furthermore, in [82], Dawes and Corrigan applied linear prediction models to tasks such as psychiatric diagnosis and predicting students final grade point average.

The first stage of building a decision support analysis model based on Z-score is to carefully identify factors that reflect the condition being assessed, which in our case is the security posture of a cloud supplier. According to Agarwal & Taffler, the predictive ability of a Z-score model can be enhanced if the factors upon which the model is built, reflect critical dimensions of the measured criterion [6]. Following its multivariate approach, each input variable should be included based on its actual predictive power and their dependent relationship to the criterion of interest [80]. The generic Z-score is a distillation into a single measure of some appropriately chosen factors, weighted and added. The power of the Z-score lies in the appropriate integration of distinct dimensions weighted to form a single performance measure.

$$Z_i = \frac{(y_i - y)}{\sigma} \tag{2.1}$$

The application of the Z-score in this study is not the same as Altman's Z-score, which is used as a financial analysis tool. The use of the Z-score (also known as the *standard score* in statistics) in our decision support model is to standardise the individual values from different sources, in such a way that they are as close to zero as possible and can be compared [176]. The application of this improper linear model to cloud supplier assessment requires the calculation of the mean and standard deviation of the supplier ratings (as shown in equation 2.1), and this helps to compare the capabilities of each cloud supplier. It measures how many standard deviations (σ), a score (y_i) is above or below the population mean (y) [140]. We apply the Z-score method of unit-weighted regression as a prediction model for cloud supplier security posture assessment, to objectively determine which of the members has the higher susceptibility to a cyber attack that is capable of adversely affecting the supply chain.

2.6.2 Delphi Method for Information Gathering

To enhance the predictive ability of our proposed cloud supplier security assessment model (i.e. modified Dawes model), and to objectively collect expert opinion on the security factors that contribute to the overall security risk of cloud suppliers, we opted for the Delphi research method. The application of a Delphi method to the development of a decision support tool is proposed as a scientific means of collecting the information necessary to rate cloud suppliers. Also, one could argue that Delphi is presumably one of the best-known qualitative research methods in use today based on how often it is cited, and it is gradually gaining momentum in the information systems (IS) community. Examples of past studies which adopted the Delphi method to elicit expert feedback includes that of El-Gazzar et al.

[94], where the authors investigated the most important issues enterprises face when making cloud adoption decisions. Also, Nugraha et al. [222] adapted the Wide-band Delphi process to understand Indonesian policymakers' requirements for state cyber-defence. Similarly, Saripalli et al. [271] who developed the QUIRC risk assessment model, utilised a modified wide-band Delphi method to collect numerical estimates for the impact of risk events. Furthermore, the research conducted by Parekh et al. [239], applied a Delphi process to rate cybersecurity topics based on importance, difficulty and timelessness.

According to Bourgeois et al. [47], the Delphi method is defined as a combination of qualitative and quantitative processes that draw on the opinions of identified experts to develop theories and projections for the future. It is a forecasting technique used to collect expert opinion objectively, with procedures that allow for anonymity over multiple iterations in a controlled manner. With Delphi, statistical analysis of group response is used to elicit and refine group estimations and arrive at a consensus [116, 200, 271]. The RAND Corporation developed the Delphi method in the 1950's [77] for gathering a knowledge base of military intelligence and experience, without the influence of politics, rank, or other bias. It has since been applied to other domains such as technology, population sciences, usability studies, environmental risk assessment and business applications.

The Delphi method is recommended in areas where the problem does not lend itself to precise analytical techniques but can benefit from subjective judgments on a collective basis [189]. It provides insights from the collective experience and understanding of an expert panel [273]. Given the scarcity of initiatives for the practical implementation of a formalised cloud supplier risk ratings, coupled with our knowledge of the impact supply chain risks have on cloud services, we have decided to engage cloud experts in developing a means of strategically assessing the risk of cloud suppliers. The work of Lang et al. [180], addressed a similar problem using a Delphi study. In their study, they polled experts on the Quality of Service (QoS) criteria for selecting cloud service providers.

The Delphi method is one of the most practical ways of gathering public opinion from a wide variety of experts distributed across different locations. It manages the risk of misinterpretation of participant response by the researcher, through its feedback mechanism. Findings from each stage of the study are sent to the respondents for reconsideration, which adds validity to the process since the experts can challenge any unusual researcher interpretation. According to Thiebes et al. [310], the key characteristics of the Delphi method are:

- Anonymity - participants make responses privately without feeling pressured by dominant individuals;
- Iteration - allowing participants to change their opinions;

- Controlled feedback - presenting feedback in the form of actual arguments or simple statistical summaries of the groups' response between iterations; and
- Statistical group response - at the end of the procedure, group judgement is (often) expressed as a median in which the extent of the participants' opinion spread may be used as an indication of the degree of consensus.

2.7 Summary

This chapter has taken an in-depth look into the different knowledge areas related to our work, to lay a foundation for the rest of the thesis. We highlighted the cloud's service and delivery models, its benefits and concerns, the differences between cloud and traditional IT risks, and how the risks presented by the cloud's global and dynamic supply chain offer a new level of challenge to stakeholders. We examined the predominant IT risk assessment methods highlighting the gaps in applying them to cloud risks.

Establishing the connection between transparency, trust and risk assessment and investigating how it plays a part in the interconnected cloud systems, we considered how the systems thinking approach suggested by Ghadge et al. [116] improve cloud risk assessment. This method requires us to conceptualise and analyse the interdependencies of the cloud service during risk assessment while making use of modelling and simulation techniques to draw the result of the assessment. Being an interdisciplinary problem, we investigated other decision support systems that could help us understand the deep roots of complex behaviours to promote sound decision-making.

In the next chapter, we present a review of the state-of-the-art in cloud risk assessment and take a deep dive into the models targeted at CSPs for assessing their cloud provisioning risks.

Chapter 3

Related Work

In this chapter, we present a review of the state-of-the-art in cloud risk assessment. Based on the findings of this review, we outline our approach to addressing the identified gaps.

The current state-of-the-art in cloud risk assessment is presented in the works of Alturkistani et al. [22] and Drissi et al. [93], where the authors classified the current cloud risk assessment approaches into five and seven categories respectively. Our survey work differ from both works in that, while theirs gives an overview of cloud risk assessment models applicable to both customers and providers based on the assessment methods (i.e. quantitative, qualitative, graph analysis and hierarchical), ours provides greater detail on cloud provisioning risk assessment models. We investigate models that are targeted at cloud providers to enable them to address the risks of designing, deploying, configuring, or managing the cloud. Our decision to tackle cloud provisioning risks was influenced by the scarcity of studies in this area, and on the practical need for cloud providers to assess security risks to assure secure cloud delivery to customers.

3.1 Cloud Risk Assessment

Thus far, and despite a significant number of scholars who have grappled with the issue of cloud computing risks [5, 59, 130, 304], there is currently no industry consensus on assessing cloud risks [149] and no standard measurement unit for cyber risk [261]. According to ISACA [320], this difficulty is down to the lack of a structured framework for cloud risk identification and assessment, coupled with the cloud's highly dynamic and flexible nature. In the absence of a standardised risk assessment framework for cloud computing, the industry has continued to use existing IT risk frameworks to address cloud risks [93, 309]. However, while the cloud faces some of the threats applicable to any information system, it also faces unique threats and vulnerabilities. Cloud risks, often involve multiple parties, including cloud providers (employees, facilities, systems), technology (interfaces, API), external attackers and other cloud co-tenants. Due to the variety of parties involved

in the delivery of a cloud service, cloud providers and customers have been known to face difficulties in assessing the risks of their cloud setup [304].

Cloud risk assessment is defined as a step by step, repeatable process used to produce an understanding of cloud risks associated with relinquishing control of data or management of services to an external service provider [253]. While still considered to be one of the most significant enterprise security weaknesses worldwide [308], cloud risk assessment covers the most critical functions of managing the risks of cloud computing and protects organisations against unforeseen disruptive events [116]. In MCS, where cloud architectures use services from more than one CSP, the challenge of risk assessment is evident. Tang et al. [305] argue that two significant problems have contributed to the relatively low turnout of cloud computing risk assessment research. First is the lack of systematic study on the whole process of cloud assessment, and second is the tendency for researchers to engage in qualitative research rather than quantitative research in addressing cloud computing risks.

The traditional IT risk assessment frameworks, e.g. ISO/IEC 27005, which were developed before the evolution of cloud computing, cannot cater to the complexity or pervasiveness of these dynamic and automated systems of systems [17]. According to Albakri et al. [19], the most common risk assessment standards assume that an organisation's assets are managed in-house, and the security management processes are compliant with the organisation's standards. These frameworks are structured based on security control domains [261]. Applying frameworks developed with these assumptions to the cloud, therefore, leads to increased vulnerabilities and inadequate implementation of security controls. Some of the other concerns often raised about the traditional risk assessment frameworks includes the shortcomings of periodic assessment, limited knowledge of the Target of Assessment (ToA), and inability to measure cyber risk in dynamic systems [15, 223, 224]. As such, the cloud industry stands to benefit from the development of conceptual models that address different cloud stakeholder needs.

Cloud risk assessment requires domain-specific knowledge and a deep understanding of the ToA, i.e. cloud service, to ensure one can arrive at reasonable risk estimates. The assessment of cloud risks relies on the expert's experience in considering and deciding on the probability of each threat event based on available real-world data and nature of cloud service. Every valuable asset has some level of exposure that will generate an impact [53]; the same way risk has a component of uncertainty and a cost [142, 172]. Some of the typical challenges of cloud risk assessment, identified in previous academic studies include: (a) lack of appropriate historical data, (b) lack of trust in the CSP and the data provided for risk assessment, (c) the dynamic supply chain of infrastructure and services, (d) immature offering from CSPs, and (e) the lack of visibility of security control [14, 22, 23, 93, 100, 261, 309].

According to Hentschel et al. [135], the perspective of the CSP is rarely discussed in the literature. Recent cloud risk assessment models (e.g., Busby et al. [54], Cayirci et al. [58] and Islam et al. [149]) have been aimed at assisting customers in assessing cloud adoption and migration risks, while others (e.g., Sendi & Cheriet [278] and Sivasubramanian et al. [289]) have followed the traditional route to security risk assessment. This traditional approach concentrates on the focal organisation, their critical assets, threats and likelihood of impact, without paying attention to the supplier network nor fully understanding its interrelated consequences. Based on the complexity of cloud service provisioning, there is, therefore, a need for more research aimed at improving cloud provisioning risk assessment.

3.2 Conceptual Models for Assessing Cloud Provisioning Risks

We define a cloud risk assessment model as a tool designed for cloud stakeholders to assess the risks they face from the adoption, creation or operation of a particular service. Conceptual models are tools composed of concepts and relationships, designed to help make sense of complex issues [146], such as those faced in cloud risk assessment. A cloud model is used to evaluate the various background information obtained from members of the supply chain and other public sources. It helps to understand the problem area, analyse various risk scenarios and improve the defensibility of risk result. The application of a well-founded risk model to cloud assessment ensures that the process follows a particular method and is repeatable, understandable and traceable. A risk model defines the risk factors to be assessed, and the relationship between them, with the factors used as input to determine the risk level during assessments. Risk factors include vulnerability, impact, threat, likelihood, probability, exposure factors and predisposing condition [258].

3.2.1 Existing Approaches

In this section, we examine a set of established service-driven conceptual models that can be used by CSPs to assess cloud risk. To identify conceptual models proposed for the assessment of cloud provisioning risks which could also serve as a reference to the cloud community, we conducted a systematic review. We adopted a three-staged literature review process similar to that of Fernandez-Aleman et al. [102]. An overview of the main stages of our systematic review is presented in Figure 3.1.

Before beginning the search, we identified the eligibility criteria to include:

1. Articles published in English (CR1)
2. Articles on cloud risk assessment (CR2)
3. Articles proposing cloud risk assessment models for CSPs (CR3)

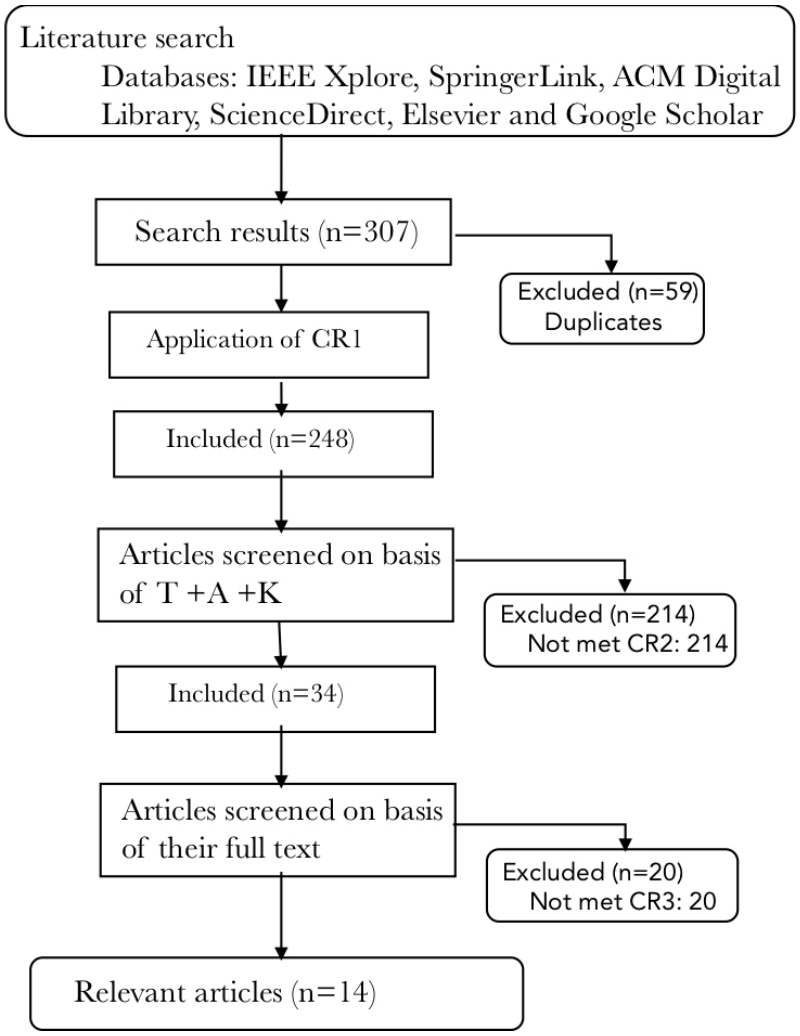


Figure 3.1: Flow Diagram of Inclusion/Exclusion and Literature Analysis Process

We considered only peer-reviewed articles, journals and conference proceeding, and limited our search to well-regarded online databases such as the IEEE Xplore, SpringerLink, ACM Digital Library, ScienceDirect, Elsevier and Google Scholar. Due to the nascent nature of cloud provider risk assessment and owing to the limited research in this area of cloud computing, we narrowed our search to articles published between 2010 and 2018. The keywords used in our search criteria included "cloud service provider risk assessment" OR "cloud provider risk assessment" OR "cloud risk model" OR "cloud risk assessment". We explored the title, abstract and keywords (T+A+K) of identified articles to determine their eligibility. Next, we carried out a partial or complete reading of the articles that had not been eliminated in the T+A+K stage, and in some cases scanned the reference list of the articles to discover new studies that satisfied our inclusion criteria.

A total of 14 articles were selected for this review. These were derived as follows. Through our database search using the predefined keywords, we were able to identify a

total of 307 studies/articles. Of these, 59 were first excluded as they represented duplicates of existing articles. Next, CR1 was applied, and all of the 248 articles passed this criterion. The T+A+K's of the remaining 248 articles were then examined, and 214 of these were discarded because they did not meet criterion CR2. While most of them contained elements of cloud risk assessment, it was not the core area of the study. The remaining 34 studies were examined in greater detail, based on partial or full reads of their text. Of the 34 articles, 20 were excluded for not meeting criterion CR3. Some of the articles excluded in the final phase of the review included that of Cayirci et al. [58], Islam et al. [149] and Tang & Liu [304]. While they discussed cloud risk assessment in great detail, they only concentrated on cloud consumer risks.

In Table 3.1, we present a cross-section of proposed cloud risk assessment methods applicable to CSP risks, highlighting their assessment method, their use of experts and evaluation of supply chain. The choice of criteria for comparison is based on the existing gaps in the use of traditional risk assessment frameworks to assess cloud risks.

In [271], Saripalli et al. proposed the quantitative risk and impact assessment framework (QUIRC) model for assessing security risks associated with cloud computing platforms based on six key security objectives (SO): confidentiality, integrity, availability, multiparty trust, mutual auditability and usability. The model was developed on the premise that most of the typical attack vectors and events, map to one of these six categories. QUIRC uses the Federal Information Processing Standard (FIPS) model (LOW, MEDIUM, HIGH) for the potential impact definition and assigns scores to the threat scenarios affecting these six security objectives (SO). It employs a modified wide-band Delphi method to scientifically collect numerical estimates for the impact of events and the degree of confidence in the probability values, to arrive at a consensus on the value of risk. Likewise, Shamelisendi & Cheriet [278] proposed a risk assessment model for cloud computing based on fuzzy multi-criteria decision-making technique and used expert opinions to weigh the impact of threat on the confidentiality, integrity and availability of an IT asset. Similarly, Liu & Liu [190] proposed an information security risk assessment model based on the analytic hierarchy process (AHP) for cloud computing environments. Using the integrated method of risk analysis, they combine qualitative and quantitative analysis methods and complement it with expert experience and objective facts to perform a comprehensive cloud risk assessment.

The EU-funded project OPTIMIS [89] also developed a risk assessment method that applies to different cloud stakeholders at various stages of the cloud service provisioning lifecycle. The risk assessment framework shows how supply chain transparency assists cloud providers in assessing the risks of their infrastructure provider (IP). The framework stresses the importance of prior service level agreement (SLA) performance, geographical

Table 3.1: Existing Cloud Risk Assessment Models

Author/ Year	Cloud Risk Assessment Description	Method	Implem-entation	Risk value	Use of Experts	Supply chain
(Albakri et al., 2014)[19]	They proposed a model that considers both the cloud customer and the CSP during its risk assessment process.	Quali-tative	Yes	Risk Matrix	No	Yes
(Chih-An & Huang 2015)[62]	Authors proposed an Adjustable Cloud Risk Assessment systeM (ACRAM) for CSPs and users. The tool assesses the risk of a cloud environment based on the historical or runtime software vulnerabilities of virtual machines or network devices.	Semi-quanti-tative	Partial	Risk Score	No	Yes
(Djemame et al., 2011) [89]	Risk assessment framework with methodologies for the identification, evaluation, mitigation & monitoring of cloud risks during the various stages of cloud provision.	Semi-quanti-tative	No	Risk Score	No	Yes
(Fito et al., 2010)[105]	A cloud risk assessment model for analysing the data security risks of confidential data. It prioritises cloud risks according to their impact on Business Level Objectives(BLO).	Semi-quanti-tative	Yes	Risk Score	No	No
(Liu & Liu, 2011)[190]	The model assesses cloud risks based on eight kinds of threats to security principles and their corresponding factors.	Quali-tative	No	Risk Score	Yes	No
(Saripalli & Walters, 2010) [271]	A quantitative risk and impact assessment of cloud risk events based on six key security objectives.	Semi-quanti-tative	No	Risk Score	Yes	No
(Sendi & Cheriet, 2014)[278]	The model uses fuzzy multi-criteria decision-making technique to assess cloud risks. Linguistic variables are used to obtain expert opinions for weighting security risk criteria.	Quanti-tative	Yes	Risk Score	No	No
(Sivasubram-anian et al., 2017)[289]	The model measures cloud risks in terms of impact, occurrence and disclosure, to arrive at a Risk Priority Number (RPN).	Semi-quanti-tative	No	Risk Score	No	No
(Zhang et al ., 2010)[334]	The framework was developed for a better understanding of critical areas in cloud computing environ-ments and the identification and mitigation of cloud risks.	Quali-tative	No	Risk Score	No	No

location, security compliance, business stability and general infrastructure, in assessing the risk of the infrastructure provider. In [19], Albakri et al. proposed a security risk assessment framework for cloud computing environments. This framework contains several components, including a cloud service provider risk assessment manager (CSPRAM). It is designed to be used by CSPs in assessing the security risks in their cloud computing environment and is complemented by the inclusion of customers' evaluation of security risk factors [19]. The model addresses the challenge of defining the risk criteria according to the organisation's security objectives and considering these criteria when evaluating the value of a risk event, by including cloud customers (CC) in the assessment process.

Some other slightly different approaches to assessing cloud provider risks include the work of Sahinoglu & Morton [263] who proposed the CLOUD Risk-O-Meter. This model operates by taking a survey of the dynamic cloud setup, assesses cloud risks based on its percentage of occurrence and also applies game-theoretic approaches to determine a cost-minimal mitigation approach. In [62], Chih & Huang proposed Adjustable Cloud Risk Assessment systeM (ACRAM) for CSPs and users, a tool which assesses the risk of a cloud based on the historical or runtime software vulnerabilities of virtual machines and network devices. Here, the risk value is presented as a score, based on the weight of the "C, I, A", requirements. Also, Basu et al. [33] proposed a semi-quantitative risk assessment methodology to assess the risks to assets and stakeholders of a cloud system. The proposed model recognises the cloud asset valuation and its physical & logical dependencies in the calculation of the risk score.

3.2.2 Limitations and Gaps

The amount of research into the assessment of cloud provisioning risks is limited. Examination of the literature relevant to cloud risk assessment so far has identified that there is more research into cloud adoption or provider selection risks [111, 149, 155, 169], compared to cloud provider risks. The lack of studies targeted at assessing cloud service provision risks has also resulted in less agile cloud environments [12]. While all of the models described in Table 3.1 were developed in the cloud era, their principally traditional approach to risk assessment, application of qualitative methods, and the limited knowledge of the Target of Assessment (ToA) make them unsuitable for measuring cyber risk in dynamic cloud environments.

Similarly, none of the models presented in Table 3.1 estimated the value of a cloud risk in monetary terms (£), which is known to promote cost-effective risk mitigation and optimal risk prioritisation [202]. Also, we see that the majority of the models adopted a silo approach to assessing risks (i.e. limiting the assessment to the focal CSP), and only three considered the inherent risks in the supply chain. Considering that CSPs rely on

a dynamic and complex supply chain, where the perceived level of the security risk of the cloud service increases with each additional component integrated into the offering, it would have been fitting for these models to assist the CSPs to understand the vulnerabilities each component supplier introduces to the cloud service. This remains a gap with provider-based risk assessment, one which if addressed, is capable of promoting visibility into the vulnerability of the chain and information sharing, both of which are key to conducting a comprehensive RA. Lastly, most of the studies failed to carry out any comprehensive validation of their models, either through making the demo tool available to the open-source community or by the conduct of real-world case studies. It is therefore difficult to judge the applicability of these proposed model for assessing cloud provider risks.

Based on the gaps identified above, our research looks to establish a niche around which cloud risk assessment can be improved. We begin by gauging expert opinions on supply chain transparency and its effect of cloud risk assessment. After which, we propose a cloud risk assessment model that will attempt to bridge some of the identified gaps, using the knowledge acquired from literature and surveys. Particular attention will be given to proposing a model that is systematic, structured, transparent and inclusive in its assessment of risk related to cloud service provision. Cloud security has generally been presented as a big black box to customers, but we believe that by breaking down a cloud service into its component services and understanding the interdependence between the components and identifying & assessing its component suppliers, CSPs can uncover any hidden vulnerabilities starting from the first tier to the lower tiers of the chain. We hypothesise that this approach will ultimately improve the risk assessment process. Therefore, as part of the study, we will conduct real-world case studies to determine if our proposed model addresses the identified risk assessment gaps.

Chapter 4

Research Methodology

In this chapter, we detail the design of the study, including a description of the study population, details of the proposed research instrument and a description of the data collection procedures.

Broadly, this study is broken into five stages. The research emerged from a qualitative study involving content analysis, survey and interview with experts on CSP supply chain transparency [11] and an extensive literature review of cloud computing risks and the supply chain of cloud services. As a result, we found out that only a few studies have investigated the effect of supply chain risks in cloud computing and far too little attention has been paid to assessing cloud risks from a supply chain perspective. To better understand the industry practices with regards to cloud risk assessment and the level of awareness of supply chain cyber risks, we conducted another survey with a broader group. This approach is in line with the use of mixed methods sequential research design recommended by Creswell and Clark [73].

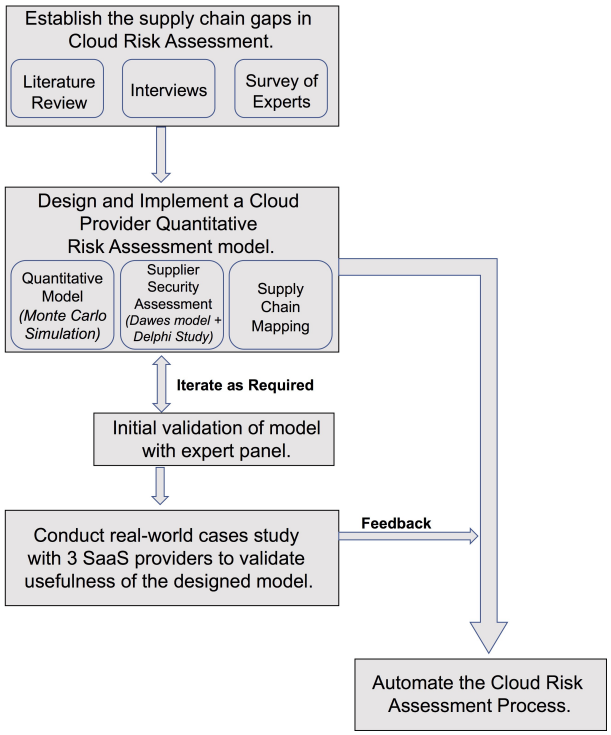


Figure 4.1: Research Methodology

Mixed method research enables the researcher to mix or combine quantitative and qualitative research techniques, methods, approaches, concepts into a single study to expand one's understanding of the subject area [160]. Its central argument is that the use of both quantitative and qualitative methods in a single study provides a better understanding

of research problems than either approach alone. It is an inclusive, pluralistic, and complementary method which draws from the strengths and minimise the weaknesses of both traditional research methods. While we considered the different mixed-method paradigmatic positions (i.e. a-paradigmatic, multiple paradigm and single paradigm), we chose the single paradigm approach to address our research questions [128]. According to [306], a paradigm is a worldview, together with the various philosophical assumptions associated with that point of view. Based on our chosen approach, we decided on the pragmatism approach over the transformative option, for two reasons. First, the pragmatism approach is oriented towards solving practical, real-world problems rather than the assumption about the nature of knowledge [128]. Second, the pragmatic approach has been advocated by several mixed-method researchers, including Johnson and Onwuegbuzie [160] & Morgan [207].

The pragmatic method provides us with a middle position philosophically and methodologically and offers us a practical and outcome-oriented method of inquiry and a method for selecting methodological mixes for answering our research questions. Its logic of enquiry includes the use of induction, deduction and abduction methods, offering researchers the best opportunities for answering their research questions [160]. Pragmatists believe that observable phenomena, subjective meanings or both, can provide acceptable knowledge to address a research objective. Therefore, seeing that our research looked to address practical cloud risk assessment gaps, the pragmatic method enabled us to fit together the insights provided by the qualitative and quantitative research methods into a workable solution [160]. While in some quarters, our choice of the mixed-method approach might appear to be vague or methodologically unsatisfactory, its success is dependent on the results of the studies, the interpretation of our findings and its practical implication to the cloud industry.

Below are the five stages of the Methodology.

Stage 1 - Preliminary work: Conduct literature review, interviews and online survey to establish a research gap.

Stage 2: Propose and design a cloud cyber supply chain risk assessment model.

Stage 3: Implement the cloud risk assessment tool.

Stage 4: Evaluate the developed tools using real-world case studies.

Stage 5: System Development of the RA web application.

4.1 Validating the Cloud Risk Assessment Gap

The participants for the preliminary stage of this study were recruited mainly through the distribution of survey recruitment calling card at cloud conferences within the UK. We also

worked with organisations such as the Cloud Industry Forum (CIF), the London chapter of the Information Systems Audit and Control Association (ISACA) and the British Computer Society (BCS), who helped to send the surveys to their members. Furthermore, we engaged in one-on-one conversations in recruiting other IT professionals, whom we considered to be cloud experts, using mediums such as LinkedIn.

As part of validating the cloud risk assessment gap, we conducted two surveys. The first considered the effect that supply chain transparency had on cloud risks. It investigated the extent of supply chain information CSPs shared with their customers and ways of improving this transparency. In the second survey, we sought to address the gaps in previous studies, which highlighted the inability of current risk assessment methods to cope with the dynamic cloud [22, 309]. We posited that this was down to the lack of consideration for the inherent risk of the supply chain. So, we conducted an industry survey to gauge stakeholder awareness of supply chain risks, seeking to find out the risk assessment methods commonly used, factors that hindered a comprehensive evaluation and how the current state-of-the-art can be improved. In the following sections, we describe our survey method and the study population.

4.1.1 Cloud Supply Chain Transparency Survey and Interview

According to Gavan Egan, vice-president of Verizon Terremark Europe, "Transparency is the biggest challenge in moving to the cloud and not security" [25]. Therefore, seeing that the lack of provider transparency and the limited visibility of CSP security controls, also adds to the growing list of cloud risks [327], our goal was to investigate how much cloud providers know about their supply chain and how much information they were willing to share with their customers.

To gain this understanding, we engaged in field research. Qualitative methods (case study, questionnaires and interviews) were chosen to allow for a more in-depth insight into supply chain risks as we get to look at the issues from different perspectives, including both customer and providers in our study. We set out to determine how providers could offer a more transparent service to assist customers with mitigating their risks while still maintaining their intellectual property and competitive advantage. Our research adopted the use of a case study, as it is a well-established approach to explorative investigation. We developed the case study for a fictitious company (Payworq), who is a SaaS provider for a payment application (Payfruit) (see Figure 4.2). Payworq hosts their SaaS application with an IaaS provider (A400), a company they selected based on its industry reputation and its promise of flexibility, reliability, redundancy and compliance to standards. Recently, the Payfruit SaaS application suffered a downtime for approximately four hours due to a power outage at A400's Internet Service Provider (ISP) datacentre. Respondents were to

assume the role of the Payworq (SaaS provider) who was conducting a post-incident review with their IaaS provider about the outage and also wanted to improve their risk assessment process (see Appendix D). The questions that followed the case study sought to establish how both cloud customer and provider risk assessment goals can be addressed. We aimed to address the following questions:

1. What information should cloud customers ask CSP about its supply chain?
2. How much should CSP be willing to share with their customers?
3. What are the risks of customers not knowing enough about the supply chain?
4. How can transparency be improved in cloud computing?

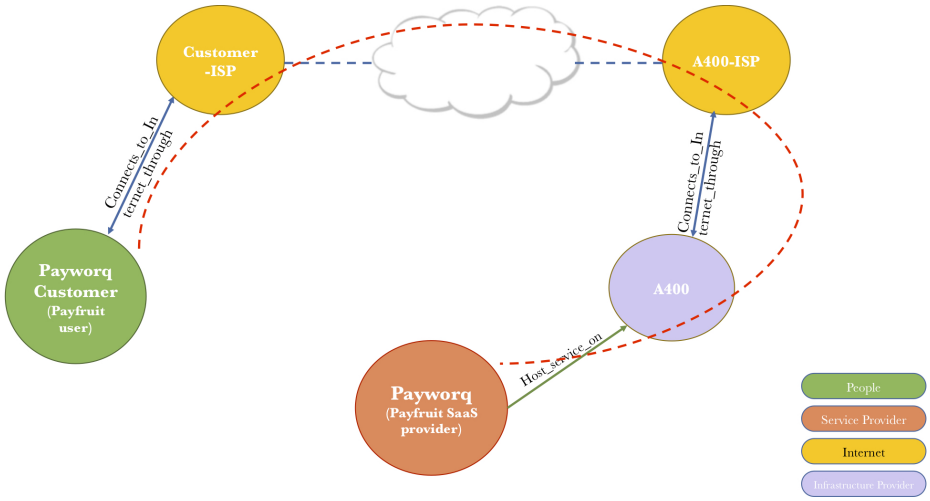


Figure 4.2: Payworq service outage due to A400 ISP downtime

The formation of the questionnaire followed an iterative process, taking literature surveys, supervisor and colleague discussions, as well as pilot feedback into account. It was approved by the Central University Research Ethics Committee (CUREC) of the University of Oxford under Reference Number: R44459/RE001)(see Appendix C). Our pilot test was conducted with four people to ensure the case study and follow-up questionnaire was adequately set up.

As a supplement to our case study, we conducted semi-structured interviews with some of the participants to discover more about their supply chain and get their views on transparency in cloud computing. We decided to conduct interviews because it enabled us to consider the personal perceptions, motives, background and experience of the interviewees in a more comprehensive and detailed way. The Cloud Expo event at the Excel Centre in London between the 12th and 13th of April, 2016, provided us with the opportunity to interact with a broad range of cloud providers. Wherever we got an audience, we often sought

to speak with the most technical representative of the cloud exhibitors who understood the cloud business and its complexities; a phenomenon often referred to as the "elite bias" [211]. Although to build a safeguard against this bias, we planned to speak with CSPs of different cloud models and of varying sizes, who we hypothesised will have contrasting opinions on the cloud supply chain.

Furthermore, since our interview was part of a qualitative research, and because of the need to establish a social context, we adopted the dramaturgical model, which builds on the general theory of using face-to-face interaction to interpret social exchanges [136]. As part of the dramaturgical approach, we took the time to introduce ourselves, explain the purpose of the interview, described the scenario, ask and discuss the key questions, and closed out each interview with an offer to provide feedback to each respondent [211]. Those interviewed were made up of SaaS, PaaS and IaaS vendors who either owned their hosting infrastructure or partnered with one of the top four cloud IaaS providers, named by Li et al. [185] as Amazon Web Services, Microsoft, Google and Rackspace. Of the 40 exhibitors we approached, 15 of them granted us an audience, with the majority of the interview conducted on the promise of anonymity. The semi-structured nature of the research also enabled us to engage the cloud providers in further conversations around their cloud offering and supply chain while also allowing us to assess their transparency.

In the course of the study and after the analysis of participants' response to the Payworq case study, we had gathered some transparency features that could be useful in comparing cloud providers on the information they published on their websites. We examined twenty-five (25) SaaS vendors, which were conveniently sampled from a list of the top 200 UK public cloud computing providers identified by Cloudscape [43]. We thoroughly examined each vendor based on the information published on their website detailing our defined transparency features. We compared SaaS providers in five different cloud service category, namely: online workspace, finance/ERP, human resource management (HRM), customer relationship management (CRM) and collaboration.

4.1.2 Cloud Risks and Risk Assessment Survey

Conducting research using a survey instrument rests on the established practice of finding things out by asking people questions, with the central ingredients of the study being the interviewer's questions and the respondent's answer [182]. Before our work, several lines of evidence have suggested that the limited cloud supply chain transparency is the reason why some cloud customers engage in simple risk assessment based on qualitative methods, and others choose to blindly trust their cloud providers without verifying the existence of security controls [29, 242, 304]. Therefore, seeing that few studies have investigated the effect of supply chain risks in cloud computing, or looked into assessing cloud risks from

a supply chain perspective, we surveyed cloud professionals to understand the industry practices with regards to cloud risk assessment and their level of awareness of cyber supply chain risks.

Based on the above, it would seem that improving cloud risk assessment methods, calls for a more transparent supply chain and the visibility of security controls. So, we conducted a survey to gauge public opinion on the cloud risk assessment problem, adapting our questions to cybersecurity professionals, risk practitioners, technical personnel and executives who are involved in the risk assessment and decision-making process of cloud services. The design of the survey was based on our need to:

1. Understand cloud stakeholder's level of awareness about supply chain risks.
2. Capture the decision-making process involved in cloud supplier selection.
3. Identify conventional risk identification/assessment methodologies employed within cloud provider and consumer environments.
4. Identify factors that contribute to the supply chain risks in cloud computing.

We limited the scope of the survey to corporate organisations instead of end-users, based on our personal experience of not assessing the risks of our cloud applications. Considering that the unavailability of a cloud service or data loss has a lesser impact on a single user than for an organisation, it is interesting to investigate how businesses address cloud risk, acknowledging the importance of data security to their mission, functions, image, or reputation. Surveys, such as that conducted by Boyson et al. [50] have also shown that the cyber supply chain lacked accountability and a chain of custody, which is often attributed to the failure of supply chain management [5]. We, therefore, used this survey to establish the problem scope and identify the current strategies cloud customer and provider organisations rely on to deter and mitigate known risks and potential threats.

The initial pool of survey questions was derived from previous research work on supply chain risks [11] as well as a thorough literature review of cloud computing risk materials from both the industry and the academic community. After considering the pool of questions, some were dropped, others were re-worded, and the remaining items were incorporated into the questionnaire. We pre-tested the questionnaire with two industry respondents and three academic researchers using the Bristol Online Survey (BOS) system. The University's ethics committee approved the study under Ref No: R50232/RE001 (see [229] for the questionnaire and Appendix C for approval).

The answers provided to some of the critical questions in this survey formed the background of our risk assessment model, particularly around the cloud supplier security assessment tool for identifying weak suppliers within a supply chain. Although this part of the

study was only meant for information gathering and to verify some of the gaps we identified during our literature review, the analysis of respondent feedback provided us with valuable data for other phases of the research. See Chapter 5 for the findings of this study.

4.2 Proposed Cloud Risk Assessment Approach

Past studies have highlighted the lack of transparency [58, 242] intrinsic to the operations of CSPs, as a hindrance to cloud stakeholders assessing their cloud risks. Likewise, our studies [11, 14], which were aimed at validating the existence of these gaps, concluded that majority of the cloud risks were linked to its complex supply chain, and urged CSPs to be more transparent, in order to help their customers objectively and comprehensively assess cloud risks. Interestingly, this lack of transparency and visibility into CSP controls is perceived as a contributing factor to the predominant use of qualitative risk matrix and ratings in conducting cloud assessment [14]. Because these methods sometimes lack any meaningful analysis or clear definitions, they often result in a poorly informed prioritisation of cloud risks [112, 167].

According to Charney & Werner [61], it is appropriate for organisations whose critical data reside in the cloud to develop a robust threat model to help identify and prioritise the supply chain risks. With the architecture of a cloud service made up of software components structured as services and involving a fragmented and dispersed supply chain, assessing the risk of a cloud service requires us to understand the vulnerabilities of the individual components to identify where the weak spots exist in the supply chain. Cloud risks vary depending on the sensitivity of the data, service & delivery model, abstraction level and security objectives [44, 93, 271]. Therefore, when assessing a cloud risk, it has become essential to include all entities and components that could potentially be involved in the attack into the assessment [44]. Also, with transparency being attributed as a significant hindrance to practical risk assessment [14, 66, 242], we look to explore the advantages of a quantitative risk assessment model, based on the use of numerical operations in cost/benefit analysis and the forms of transparency they produce [129].

We propose a structured framework which is based on the quantitative risk assessment method and is supported by supplier security assessment and supply chain mapping in the identification, analysis and evaluation of cloud risks. While the cloud supply chain is indeed dynamic, our proposed model follows a static approach and is designed to illuminate the risks of the cloud supply chain to CSPs. Targeting SaaS CSPs, the plan is for the model to follow a systematic approach to cloud risk assessment, decomposing a cloud service into its component services, mapping its supply chain, and using a multi-criteria decision support tool to assess the cybersecurity posture of the suppliers [14]. This approach reflects the systems thinking method described in section 2.5 and attempts to bridge the supply chain

gap identified in section 3.2.2. The systems thinking approach requires us to conceptualise and analyse the interdependencies of a cloud service during risk assessment while making use of modelling and simulation techniques to draw the result of the assessment [116]. While not ignorant of the counter-argument against quantitative models, particularly around their complexity of computation, method of measurement, cost (expert time and effort) and subjective confidence (over/under) in estimating risk factors, we look to investigate how such analysis can be carried out by calibrated in-house experts with the knowledge of the cloud service, its supply chain and probable risks. This involves complementing the expert intuition with a clearly defined and structured quantitative mathematical model to deal with the variation of uncertainty.

Acknowledging that the methods of communicating cloud risks have also not improved significantly in the last decade, we identify the need for a more sophisticated and data-driven process, where the value of a cloud risk is based on the decomposition of a risk scenario into its various risk variables and the risk value expressed in monetary terms. We aim to present the CSP's cloud risk in a format that is consistent, repeatable, traceable and understandable, one which encourages proactive mitigation of cloud risks. It also helps to justify significant security investments to decision-makers. Our proposed model builds on existing risk assessment standards and guidance documents such as ISO/IEC 27005:2011, ISO/IEC 31000:2009, NIST 800-30v1 and FAIR risk assessment. Although due to their broad applicability, some of these popular RA/RM frameworks, describe risk assessment at an abstract level and do not offer sufficient practical guidelines for completing each step, we improve on their processes by integrating supply chain mapping and supplier security assessment modules into the risk assessment process. We included these tools, on recognising that the responses CSPs got from their annual supplier questionnaire, did not highlight which of the suppliers presented the most risk to the cloud application. Also, we identified the immense value the pictorial representation of a supply chain, and the results of a supplier cyber posture assessment add to the 'a priori' knowledge of the individual estimating the risk of the cloud service.

For the implementation of the model, we propose the use of a graphing database application(Neo4j) for the supply chain mapping [214], Z-score model (Dawes model) for the supplier cyber posture assessment (see section 2.6.1) and the Monte Carlo simulation for the quantitative risk analysis piece. In deciding on which tool to use for the supply chain mapping, we considered several visualisation tools including Sourcemap, Achilles and Cytoscape, but decided on Neo4j because of its in-built graph database capabilities. With regards to the quantitative risk analysis, we examined several approaches including using a probabilistic logic sampling with Bayesian Network [134], seeing that Bayesian belief networks are capable of representing uncertain expert knowledge in coherent probabilistic form. Also,

we considered the use of a deterministic modelling approach such as the Point Estimate Method (PEM), where we could represent our uncertain input variables with "best guest" estimates [323]. This method enables us to replace probability distributions of continuous random variables with their discrete equivalents of best, worst, or most likely values. However, despite its simplistic nature, we decided against adopting this approach due to the insufficient historical cloud risk data available to stakeholders and our unwillingness to give equal weight to expert estimates due to the inherent uncertainty in estimating an unknown value.

Based on the above, we decided on the Monte Carlo method due to the ease of its simulation, its computational efficiency, extensibility and flexibility. The Monte Carlo simulation is a computerised mathematical technique that allows people to account for risk in quantitative analysis and decision making [234]. It is a stochastic modelling tool which is used to provide estimates for complex problems where there are significant uncertainty [112, 161]. According to Hastie [131], this uncertainty is based on decision-makers' judgement of the propensity for each identified event to occur. Monte Carlo carries out a random sampling of uncertain risk variable inputs to generate a range of possible outcomes for each risk scenario, with a confidence measure for each outcome. By using a range of possible values, instead of a single guess, Monte Carlo simulation helps to create a more realistic picture of the value of the risk, by providing the output values as a range. This provides a better understanding of the risk and the uncertainty in the model. For example, service disruptions and adverse actions in the supply chain (as a random event) can be simulated using repeated random sampling to produce a probability distribution of possible risk results.

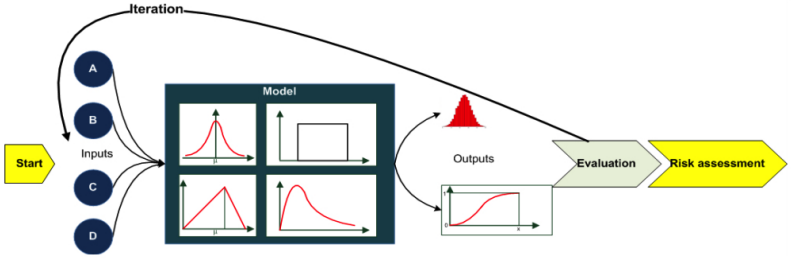


Figure 4.3: Monte Carlo Simulation Process. This figure has been taken from [276]

As shown in Figure 4.3, the Monte Carlo simulator receives the estimated risk factors as input and based on the predefined model, generates risk scenarios through a random number generator over multiple iterations (e.g. 100,000). It calculates the risk value over this number of iterations, each time using a different set of random values from the probability functions and at the end producing a distribution of possible risk values for a particular risk item [234]. The number of simulations conducted and the number of iterations in each simulation is a matter of the confidence measures associated with the results [92]. However,

to avoid the delay associated with computing too many samples, we settled for five (5) simulations of a hundred thousand (100,000) iterations each, a combination that proved to be sufficient for our model. With the Monte Carlo simulation, we can run different scenarios of the risk estimates to make reasonable estimates. Applying Monte Carlo simulation, each expert makes an independent estimation of the probability, frequency, impact cost and evaluation of countermeasures for each risk item, which is then combined to generate the estimated value of the risk (£). While the scoping part of the work and selecting the appropriate probability distribution is where the challenge lies, the running of the Monte Carlo simulation is relatively straightforward.

In conclusion, given the scarcity of initiatives for the practical implementation of a quantitative risk assessment of a cloud service, our proposed model contributes towards improving the state-of-the-art knowledge around the transparency of the cloud supply chain, cyber supply chain risks, supply chain mapping and the quantitative risk assessment of cloud services. While numerous scholars have openly questioned the subjectivity of experts' estimate in quantitative analysis [258, 309], our proposed model aims to show that despite the lack of historical data, cloud risk assessments can achieve increased objectivity through the use of controlled experimentation, clearly defined model, peer reviews and calibration of the expert judges [112, 143].

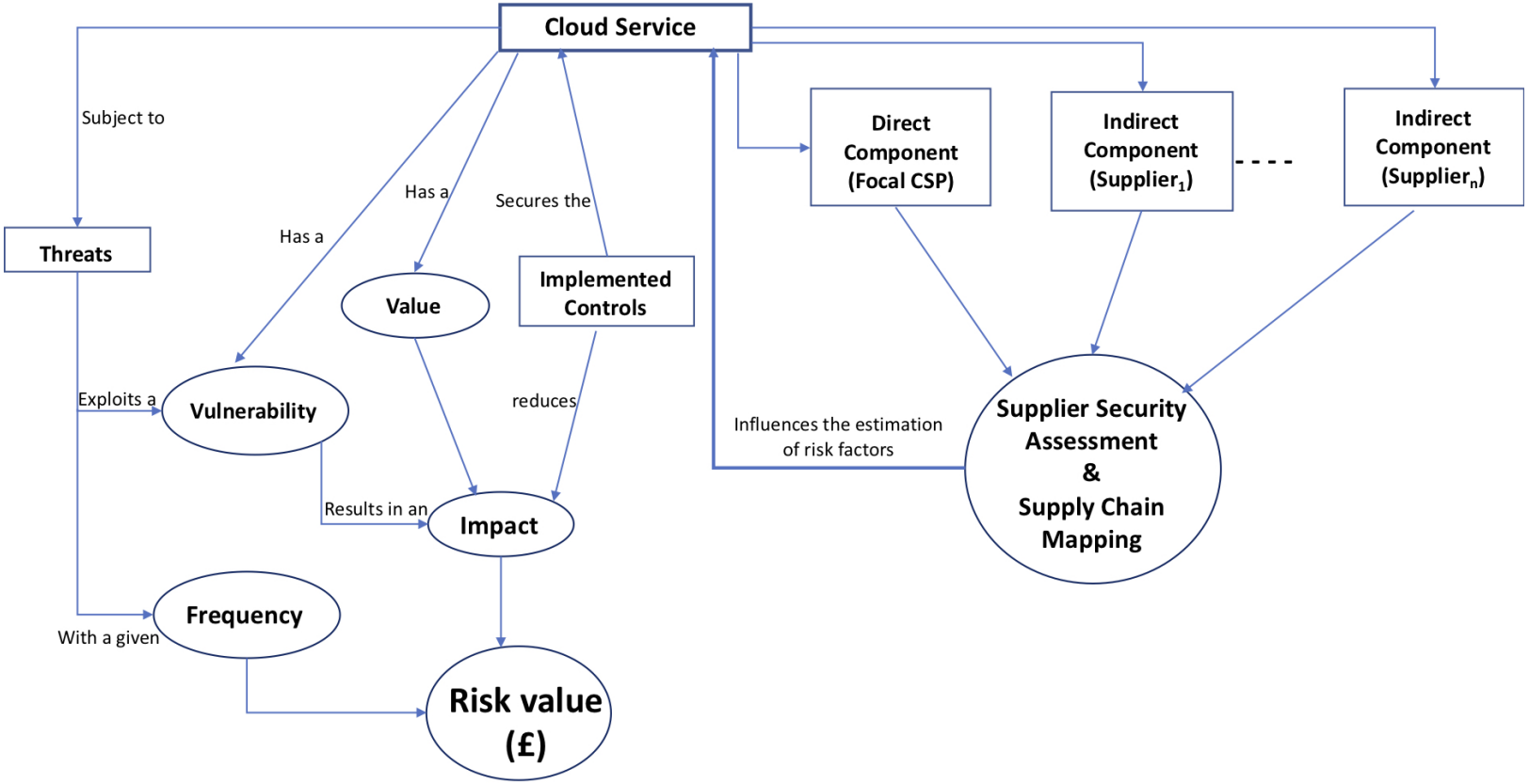


Figure 4.4: Conceptual view of the proposed framework

4.2.1 Delphi Study for obtaining Security Factors for Supplier Assessment

Our past study has shown that when selecting a cloud vendor, cloud stakeholders prioritise service suitability, vendor reputation, functionality and cost, over assessing the risk of the service [14]. Academic research also shows that majority of the cloud-specific risk assessment models [19], overlook the risks of service provision and concentrate on consumer-related risks, e.g. privacy and cloud migration risks. Furthermore, despite best intentions from the cloud security research community [267], there is no widely accepted framework or standard with appropriate metrics for assessing cloud provider and suppliers. Therefore, seeing that one of the components of the proposed model is the cyber posture assessment of cloud suppliers and that being an MCDM problem with a relatively small body of literature, a Delphi method was appropriate.

The focus of the cybersecurity posture assessment tool is to identify the weak links in the cloud provision supply chain. Therefore, it is imperative to choose a set of security factors that contribute to the overall security risk of cloud suppliers. Using the Delphi method, we sought to identify security factors that should be considered in rating cloud suppliers. These factors are ideal for the decision support model because they are widely agreed upon by the consensus of cloud experts as indicators of cloud supplier security. Considering this is a nascent area of cloud research, where there are no widely accepted frameworks or standards, judgemental information is indispensable. Conducting this study requires the dynamics of consulting with experts who have varied opinions on cloud risk assessment and ensuring that the outcome reflects the agreement of experts opinion.

4.2.1.1 Research Design

In this study, we adopted the online Delphi approach, seeing that the traditional Delphi is often criticised for its long study durations and high panel attrition. In the online Delphi, communication with experts, questionnaire design and delivery, and administration, are accomplished through the Internet [210]. This approach was taken to ensure the tenets of the Delphi study, i.e. anonymity, flexibility, iterative feedback and idea refinement, could be achieved in a controlled manner. Also, the approach allowed the experts to complete the questionnaire asynchronously, with each expert receiving the same questions and instructions. While this is potentially the right decision, we could have addressed some of its limitations if we applied the Real-time (RT) Delphi method introduced by Gordon and Pearse [120]. Although, due to the lack of ready-to-use software tools, this might have introduced a different set of challenges.

The survey instrument was designed to be self-administered by the respondents and was built using the Bristol Online Survey (BOS) tool (now Jisc online survey). The study was

conducted between January and April 2018. Taking a systematic approach, we followed the guidelines suggested by Okoli and Pawlowski [226] in the design of this study and the selection of its participants. The invitation letter, which was sent to a wide range of audience solicited for the participation of industry and academic experts in the cloud computing, supply chain and risk management fields. The invitation contained a broad view of the research aim, a brief introduction to the research method (Delphi) and some eligibility criteria, which we envisaged would restrict participation to only experts who had the right knowledge of the subject matter. The invitation was sent by e-mail to experts who had participated in previous surveys, cloud industry members known to the research team, and was posted on cloud expert forums on LinkedIn. Also, we collaborated with the Cloud Industry Forum who also sent out the invitation letter to their members. In the invitation letter, potential participants were informed of the plan for the study to be conducted over three iterations to enable us to reach consensus, and we requested that they commit to taking part in all three rounds. We decided to limit the rounds to three because, according to Turoff & Linstone [189], further iterations of the Delphi study tend to result in a few significant changes. Our eligibility criteria requested that for participation in the study, each expert should have been involved in one or more of the following activities:

- Selecting supplier for a cloud service
- Information security risk assessment
- Mapping the supply chain/ value chain of a cloud service
- Threat modelling and attack surface analysis
- Governance, Risk and Compliance

Panel members were recruited in January 2018, and following the screening and confirmation of participation, we sent out the link to the first-round questionnaire to e-mail addresses provided by the fifteen (15) cloud experts. As part of the first-round questionnaire, we re-introduced the research to the virtual panel of experts and tasked them with the difficult question of identifying security factors for cloud supplier assessment. We presented each expert with a supply chain scenario (see Appendix D for questionnaire) and tasked them with providing at least seven (7) security criteria they will consider in assessing the risk of the suppliers involved. The questionnaire was built as a scenario and was furnished with a supply chain map to allow experts to visualise the situation and suggest solutions. See Figure 4.5 for the iterative steps followed in this study.

In the second round, each panellist received a second questionnaire where they were asked to review the summarised list of security factors. This stage involved the ranking of

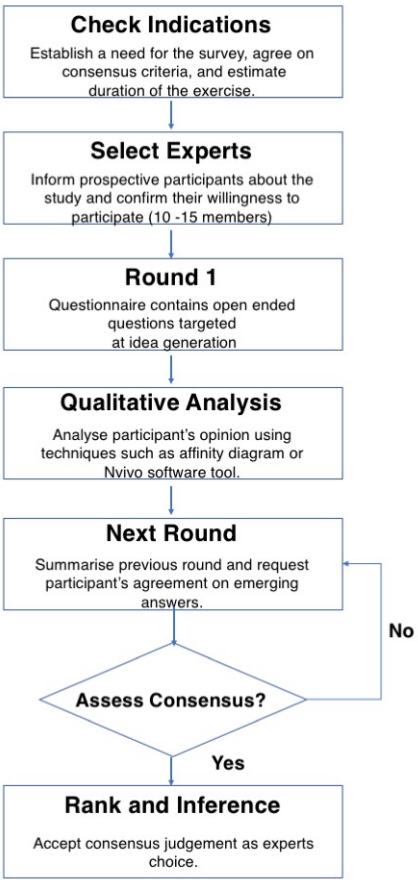


Figure 4.5: Iterative steps taken during the Delphi study

each security factor to establish expert preference and begin the assessment of consensus. We defined consensus using the Interquartile Range (IQR) based on the technique introduced by Rayens & Hahn [250]. The IQR is the absolute value of the difference between the 75^{th} and 25^{th} percentiles. Based on our projected size of the expert panel (10-15 members), we defined an IQR of 1.00 or less and a mean of 8.00 and above, as an indicator of consensus.

In the third round of the Delphi study, the convergence result of the second round was individually presented to the cloud experts using a questionnaire developed using Microsoft word which was also coded with each expert's alias and sent to them by e-mail. Indicating the current level of consensus, Delphi panellists were given a final opportunity to revise their scoring and make further clarifications on security factors that have not achieved consensus. The panel members were required to send the completed questionnaire back to the researcher for final analysis. On completing the review of the third round, all participants were sent a definitive list of the security factors and contributing elements that achieved consensus as part of this study.

Before commencing this Delphi study, ethical clearance was sought from and approved by the University of Oxford ethical approval committee. The approval was given under Ref No: R54943/RE001 for this study involving external participants (see Appendix C for CUREC approval letter).

4.3 Case Study for Proposed Model Validation

Bearing in mind that one of the limitations of existing cloud risk assessment models is that many of the proposed models remain in the prototype realm, and provide no real measurement of their effectiveness when applied in real-world scenarios [113], we chose to validate our model. Considering the plethora of research strategies available to us, which includes: survey, case study and experiment, the approach that provided the most value in answering our fourth research question (RQ4), was the case study method. RQ4 seeks to understand the applicability of the proposed model in a CSP environment and how the proposed model compares to other existing methods. Based on the taxonomy in [272] & [331], the combination of explanatory and descriptive case study research method was found to be ideal.

Robert K. Yin [331] defines the case study research method as an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundary between phenomenon and context are not visibly evident. This intensive process requires employing multiple methods (interview, observations, questionnaires and access to written documents) to gather information from one or more entities, e.g. people and groups [166]. While we have the choice of either single or multiple case study, our research design opted for the multiple case study approach, seeing that it provided us with more insight into the usefulness and effectiveness of the model in assessing cloud risks in different cloud provider settings. Also, our choice of a multiple case study approach is targeted at helping us achieve a careful and contrasting comparison on how cloud providers with potentially different supply chains apply the proposed model [331]. According to Benbasat et al. [40], evidence from two or more sources also helps to support research findings. Being an exploratory research in a relatively new area of computing, the case study research method was chosen to help the researcher gather an in-depth understanding of how cloud providers carry out risk assessments using the proposed model in a natural setting, where participants behaviour cannot be manipulated [40, 331].

Although critics of case study research maintain that the study of a limited number of cases does not offer ground for establishing reliability or generality of findings, researchers have continued to successfully apply it in carefully planned studies of real-life situations, issues and problem [294]. In the context of this research, we followed the suggested techniques for organising and conducting a case study proposed by Sue Soy [294]. We also

applied rigour to the research process by adapting the approaches suggested by Lincoln and Guba [187]. We put processes in place to promote the credibility, dependability, confirmability and transferability of the case studies. Some of the activities carried out include keeping an audit trail, describing the original context of the research, prolonged engagement with case organisations, data triangulation, providing case organisations with a risk assessment report and requesting participant feedback.

The six steps suggested by Sue Soy for conducting a case study research were drawn from the works of well-known researchers like Robert E. Stake, Helen Simons and Robert K. Yin, and they are as follows:

1. Determine and define the research questions
2. Select the cases and determine data gathering and analysis techniques
3. Prepare to collect the data
4. Collect data in the field
5. Evaluate and analyse the data
6. Prepare the report

Implementing a risk assessment model without a measure of its capability does not assure its effectiveness. Therefore, for each case study, we opened up the workings of the model to critical review by technical and business professionals who know the intricacies of managing, supporting and assessing the risks of cloud applications. We adopted a participatory research method, where both the researcher and the business and technical stakeholders within each of the SaaS companies, sit down to review their cloud service supply chain, assess its weak spots and evaluate the risks. According to Bergold and Thomas [41], the participatory research is a process that evolves when two spheres of action: science and practice - meet, interact and develop an understanding of each other. Our application of this participatory approach to the case study connects us with the empirical reality of the cloud supply chain and helps us to establish trust with the CSP, which gives us access to sensitive information about the cloud application.

In recruiting case organisations, we leveraged our existing relationships with respondents to our previous studies and requested that where it was not directly applicable to them, they should help extend the invitation to their clients and partners using the snowball sampling technique. Our invitation highlighted the novelty of our model, its benefits and our hypothesis on how the application of a rigorous and systematic approach to cloud risk assessment provided CSPs with a deeper understanding of their risks. We also included in the invitation, a poster which provides more detail on our research, progress made and

publications (see Appendix C). The CIF, an organisation which boasts of a large membership of CSPs also assisted us in getting this invitation out to their members. Each case organisation was assured of anonymity and aggregation of data as part of our reporting [40]. This approach complies with the ethical approval for this study, given by the University of Oxford Central University Research Ethics Committee, under Ref No: SSD/CUREC1A CS_C1A_18_026 (see Appendix C).

4.4 Developing the Risk Assessment Web Application

In scoping our research output, we identified the need to develop the proposed model into a web-based software for easy accessibility by cloud stakeholders. This phase was completed after the case study exercises, where we got valuable feedback on the model. For the case study, we developed a simple prototype that mirrored the functionality of the model. This prototype was an integration of spreadsheet programs and commercial off-the-shelf (COTS) applications. This, according to Sommerville [292], was sufficient for the proof-of-concept phase.

Seeing that our goal is to host the software in the cloud, we adopt the software engineering approach outlined by Sommerville [292], where the author identified four key activities that should take place during the software development lifecycle. They include:

1. Software specification: defining the details of the software and the constraints of its operation.
2. Software development: designing and programming the software.
3. Software validation: checking that the software meets requirements.
4. Software evolution: modifying the software to reflect changing customer and market requirements.

For the development of the CSCCRA web-based application, these four activities were conducted in a sequential fashion beginning with the software specification. Since we already had a prototype, which was used for conducting the case study, we had a good grasp of our requirements for the software. We improved the specification based on the feedback from the face-validation with experts and case study. Our initial prototype was an integration of a graphing database application for the supply chain mapping [214], Microsoft Excel-based Z-score model for the supplier cyber posture assessment (see section 2.6.1) and the @Risk software for the Monte Carlo simulation (quantitative risk analysis piece). This tool was sufficient for the case study stage, but to make the tool more accessible to a broader audience, we identified other areas where the software could be improved.

There are, therefore, five essential high-level requirements that this system must meet:

1. The developed system shall have an intuitive user interface that promotes easy navigation through the application.
2. The developed system shall be able to map cloud supply chains based on user input.
3. The developed system shall reliably compare the security posture of cloud suppliers.
4. The developed system shall be able to store a list of cloud risks and calculate their risk values, following user input of risk factors.
5. The developed system shall be able to store risk assessment result for future reference

The software design phase of software development lays the groundwork for a system and begins the process of converting the specification to an executable system. According to Sommerville [292], software design is a description of the structure of the software to be implemented, the data models and structures used by the system, the interfaces between system components and, sometimes, the algorithms used. Using the information from our working prototype (not web-based), we had a good head start on this critical undertaking. Figure 4.6 presents a high-level architectural view of the web application.

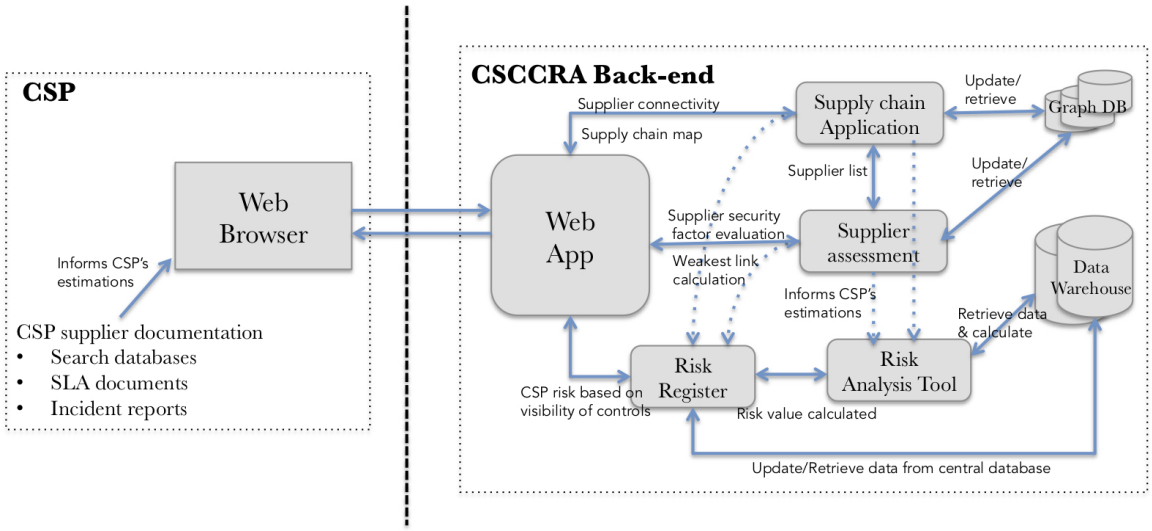


Figure 4.6: CSCCRA web application architecture overview

To implement the functionalities outlined in the design above, we had to decide on the development platform that best meets our need. We considered programming languages which the researcher was familiar with or could quickly learn. We adopted the reuse-oriented software engineering approach [292], on realising the broad base of reusable software components and the available integrating frameworks that can be used to fulfil our software design. Due to the vast array of predefined functions available in the Python programming language for Monte Carlo simulations [231], and the smooth integration of Python with the

Hypertext Markup Language (HTML) using web frameworks such as Flask or Django, we decided to develop the software using these tools.

The developed system was initially evaluated in a focus group setting with computer science researchers before the real-world evaluation with one of our case organisations. While common issues in information systems include security, usability, privacy, and maintaining data integrity [292], our initial validation of the software was based on its functionality, usability and data integrity. The evaluation was in the form of a questionnaire, where participants evaluated the capability of the software, ease-of-use, layout and interface navigation, usefulness and its ability to support decision making.

4.5 Resource Requirements

The following resources were used to conduct this multi-staged research:

1. Hardware - laptop, printer
2. Software - @RISK v7.6 Monte Carlo simulation tool, Neo4j graphing database tool, Microsoft office suite, Microsoft SQL database, Python and HTML.
3. People - Cloud Service Providers, Cloud Customers, Cloud Organisations (e.g. CIF), Information security community (e.g. ISACA), academics and colleagues.
4. Online Resources - Technology lookup website (builtwith.com), Google, Research databases, Google forms and Bristol online survey (now Jisc online survey).

4.6 Summary

In this chapter, we presented our research methodologies, which is a combination of qualitative and quantitative techniques, appropriate for our desired metric. We adopted mixed method research because it provided us with a better understanding of the research problem. The coherent narrative of our studies starting with the literature review, surveys, interviews, Delphi study and case study, confirmed the appropriateness of our chosen techniques. For each study, we sought and received ethical clearance from the University's ethical approval committee.

Here also, we described the fundamentals of our proposed model and how it addresses some of the gaps identified in the previous chapter (see section 3.2.2). Lastly, to promote the adaptability of the model to different cloud environments, we have outlined our approach for building the framework into a risk assessment software.

Chapter 5

Preliminary Results and Findings

In this chapter, we discuss the results obtained from our preliminary surveys and interviews.

The surveys whose responses form the basis of this discussion were designed to address the gaps we identified from our review of the literature. First, the survey on cloud supply chain transparency showed the existence of information asymmetry, which some would argue is less detrimental to large enterprises, who have a higher number of skilled workforce. In the interviews, we found out that the transparency of the supply chain is a customer-driven process, but the CSPs could do more to make information available and usable. Collectively, the study found that despite the genuine risks of supply chain transparency, CSPs owed it to their customers to provide easy-to-understand details on basic transparency features such as security controls and datacentre location, which could boost customer confidence and reduce perceived risks.

Next, the analysis of the survey dataset on cloud risk assessment methods & supply chain showed the lack of flexibility of the popular qualitative assessment methods in coping with the risks associated with the dynamic cloud supply chain. Likewise, the survey identified the lack of cloud provider transparency as the top hindrance to a comprehensive risk assessment.

5.1 Surveys and Interviews

5.1.1 Cloud Supply Chain Transparency

This study was carried out between March and June 2016, and it includes a case study-based survey, semi-structured interviews and a cloud provider transparency comparison.

5.1.1.1 Case Study-based Survey

The case study (see Appendix D), was sent to a total of 47 contacts, which were made up of Cloud and IT industry experts, but only 12 of them responded, giving us a response rate of 25.5% over the three months. The twelve responses received were of a good standard, judging from the level of analysis of the case study that was carried out by each of the

respondents. The two questions we required respondents to answer were based on a fictional story, and they sought to investigate what information Payworq (cloud customer) should ask the CSP, and how much information A400 (CSP) should be prepared to share with Payworq about its supply chain.

This study found out that it is vital for CSPs to share a certain level of information with their customers, irrespective of size. The reason for this is that SMB customers have often found it challenging to get CSPs to respond to their request for information (RFI), a phenomenon they put down to their limited purchasing power. Interestingly, and according to a World Bank research, SMBs accounts for 95% of existing businesses and their products and services make-up around 49.8% of the global economy [35]. However, it would seem that due to the hurdles customers go through when finding out information from CSPs, they appear to have neglected supply chain provenance, emphasising more on functionality and cost of the cloud service. From the case study, we see that the downtime suffered by Payworq prompted them to inquire more about A400 Ltd's supply chain, as they were unaware of the CSP's single source ISP. This suggests that no proper due diligence was performed. While this was a fictional story, we found this behaviour to be popular among cloud customers. It is therefore not surprising to see CSA list insufficient due diligence, among the top threats of cloud computing [58]. Raj Samani [248] in his support for the need for customer due diligence points out that, "if you cannot be sure how your data will be treated, and that it will be adequately protected, then it would be reckless to go blindly into the cloud, even if the economic benefits look attractive".

Furthermore, the response from our participants elicited a range of ideas. Over half of the replies contained the need for the cloud customer to have a high-level understanding of the architecture of the CSP's infrastructure. One of the participants commented: *"The underlying infrastructure provider should not be a secret, and CSP should be willing to share high-level details of their architecture and dependencies on third-party providers"*. Zhang et al.[334] established a correlation between the security risk associated with cloud delivery and its cloud architectures and security controls. Another compelling aspect of our respondent's feedback was the definition of service level agreement (SLA). Eight of the respondents requested the CSP to provide further details on their SLA with regards to the outage and onwards support. One respondent suggested Payworq to *"get an understanding of the CSPs uptime record as well as SLA, as this helps Payworq in setting their own SLA to their customers"*.

Some of the other information highlighted by the respondents are listed as follows:

1. **Monitoring and Notification capabilities:** According to Lee Newcombe [218], customers should trust their CSPs ability to implement adequate monitoring and

event management. One respondent mentioned that: *"CSPs should concentrate on procedures for notifying clients of problems rather than detailed internal operation".*

2. **Certification and Audits:** Respondents encouraged customers to ask CSPs for the professional and third-party certification of their operations. One respondent suggested that CSP audits should include independently verified audit reports such as the Service Organization Control (SOC) 1 and SOC 2 Type II reports.

3. **Security Controls:** In addition to the high-level architecture, the majority of case study participants believe customers need to know about security controls implemented by the CSP to protect their data. These controls include physical security, network security and application security.

On the subject of how much CSP should be willing to share with their customers, 75% of the respondents were in support of information sharing. Respondents suggested that the CSP should be prepared to tell as much as the customer will understand. Another respondent referenced the notion of providing customers sufficient information to assess their risk, stating that: *"the exact topography and schematics do not need to be shared, but A400 should be prepared to discuss where their solution has a reliance on a 3rd party, e.g. Rackspace".* In analysing the other responses received, we identified that about three of the respondents were against full disclosure of the CSPs supply chain. Another perspective of supply chain transparency paradigm is that of trust. One of our participants in relating trust to the case study believes that the CSP needs to give its customers enough information to build or retain trust; otherwise, they risk losing them following an incident. He went further to say that coupled with providing clients with high-level architecture, redundancy and security control information, CSPs can also share with their customers, their process for choosing a supplier.

In summary, the case study gave us a good foundation in this exploratory research into the effect of transparency in reducing supply chain risks in cloud computing. The participants' feedback provided us with some transparency features (security controls, architecture, SLA, Disaster Recovery (DR)/Business Continuity Plan (BCP), IT certification, technology partners), which we used in comparing CSPs on their supply chain transparency.

5.1.1.2 Interview Results

In this section, we discuss the findings of the data collected through in-depth semi-structured interviews with cloud vendors. A total of 15 informal interviews were organised around a set of predetermined open-ended questions, with other issues emerging from the response provided by the interviewee. While many of the questions were similar to that of the case study, we went into greater length in discussing participant responses. We also asked

questions about their supply chain and their awareness of supply chain risks. For the interpretation of the interview data, we carried out a qualitative content analysis, as a way of gaining access to the subjective perceptions of the interviewees [106].

When asked how much they knew about the supply chain, the responses were mixed. Initially, there was a general misconception around the definition of the supply chain, which led many of the vendors to consider themselves as their own suppliers. We corrected this notion in subsequent interviews by defining the supply chain, according to Wisner et al.'s [330]. One of those interviewed was the CEO of an original equipment manufacturer (OEM) for a private cloud infrastructure, and in our conversation, we gathered that although the product was assembled in the UK, the components were sourced from a major supplier in China. When asked, if there was a contingency in place, the answer was affirmative, but he admitted that since *they lack the visibility into the 2nd, 3rd and 4th tier suppliers, there is no guarantee that both major supplier's arrangements are not dependent on similar sub-suppliers.* Furthermore, we gathered from some of the start-up firms that *traceability most times come at a premium, which they were not willing to pay.* One interviewee cited a few examples of companies which started as a small start-up and later progressed into large firms, saying companies only start to care about the risks of the supply chain as their customer base increases, or when reliability or security issues can lead to a reputational loss.

When asked why some CSPs did not prioritise supply chain risks or the general risks of cloud computing, the interviewees pointed out that although they thought about it, it is hard to assess a worst-case scenario. One respondent added that: *"the fact that no major event resulting in multi-billion dollar loss has happened in the cloud does not mean one will not occur shortly, but we do not know any better".* This hypothesis supports the observation by New & Brown [216] concerning how the Japanese earthquake of 2011 changed the perspective of manufacturing organisations to supply chain risks. Perhaps, it will take a significant breach or downtime to one or several cloud giants before the cloud community can be awakened to the realisation of the complex commercial interdependencies that exist in cloud computing and its resultant risks, a point also echoed by Pearson et al. [243] [2].

With regards to the issue of trust, which according to Das & Teng, has a link to the level of control one has over a cloud service and the perceived risk, one of our interviewees pointed out that the situation of transparency and trust is a catch-22. He said, *"If I tell you, you might know my weakness. If I do not say, you do not trust me".* According to Akkermans et al. [18], there is a feedback loop, whereby the increase in trust leads to

[2]This significant level of event seems to have now happened if we consider the number of CSPs and corporations that were affected by the AWS S3 outage experienced in the US-EAST-1 region on the 28th of February, 2017.

an increase in transparency, which improves decision-making quality and improves supply chain performance.

In conclusion, the interviews confirmed the general lack of due diligence by cloud customers. Many of the CSPs confirmed that most customers do not ask enough information about the cloud service or its supply chain because they are more concerned about the cost and functionality. Also, we learnt that the reason many customers use the "Big four CSPs", instead of the smaller public cloud providers was that, they paid less attention to where their data was stored or who had access to it, and because the "Big four" had a good reputation. However, for the CSP, there is an incentive to establish trust with their customers, and this can happen when they provide them with the needed information. Overall, except for two interviewees, all others were in support of more cloud provider transparency, both through their online presence and in their day-to-day communications with their customers.

5.1.1.3 SaaS CSP Comparison

The many success stories of SaaS applications have demonstrated the relative ease at which start-up companies can launch a cloud service, with no upfront cost and within a few months' boasts of a sizeable customer base. Therefore, our focus was to compare SaaS providers, whose services could potentially be bought online, by a new customer who relied on the public information available on CSPs website. Talluri et al. [303] discussed how traditionally, vendor evaluations have been founded on financial measures with less emphasis on other tangible or intangible criteria but how this trend has changed, leading to the use of methodological developments in vendor evaluation techniques. The methodological approach evaluated vendors based on the consideration of multiple measures that often included product and service-related attributes [303]. We applied this methodological approach in our comparison of CSPs and centred our comparison of eight transparency features, namely:

- Architecture
- Technology/Partners
- Datacentre location
- Security features
- IT-related compliance certifications
- Advertised Service Level Agreement (SLA)
- Disaster recovery/ business continuity
- Monitoring/Support

SaaS Cloud Provider comparison based on Transparency feature											
SaaS Cloud Provider	Architecture (Yes/No)	Technology/ Partners (Yes/No)	Data center location (Yes/No)	Security features (Yes/No)	IT-related compliance certifications (ISO 27001, PCI-DSS, ITIL etc.) (Yes/No)	Other cloud offering (PaaS, IaaS & Others)	Private, Public, & Hybrid	Advertised Service Level Agreement (SLA) (Yes/No)	Disaster Recovery/ Business Continuity (Yes/No)	Monitoring/Support (Yes/No)	Scoring (No. of Yes) Maximum=8
Online workspace sub-group											
CSP1	Yes	Yes	Yes	Yes	Yes	IaaS and PaaS	All	No	Yes	Yes	7
CSP2	Yes	Yes	Yes	Yes	Yes	IaaS	All	Yes	Yes	Yes	8
CSP3	No	Yes	Yes	Yes	Yes	IaaS and others	All	No	Yes	Yes	6
CSP4	No	Yes	Yes	Yes	Yes	IaaS and others	All	Yes	Yes	Yes	7
CSP5	Yes	Yes	Yes	Yes	Yes	N/A	All	Yes	Yes	Yes	8
Finance/ERP sub-group											
CSP6	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
CSP7	No	No	No	Yes	No	N/A	public	No	No	No	1
CSP8	No	Yes	Yes	Yes	Yes	IaaS	All	No	Yes	Yes	6
CSP9	No	No	No	No	No	N/A	public	No	No	No	0
CSP10	,No	No	No	No	No	N/A	public	No	No	No	0
Human Resources (HR) sub-group											
CSP11	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP12	No	Yes	No	Yes	No	N/A	public	Yes	No	Yes	4
CSP13	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
CSP14	Yes	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP15	No	No	No	No	No	N/A	public	No	No	No	0
Customer Relationship Management (CRM) sub-group											
CSP16	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP17	Yes	Yes	Yes	Yes	Yes	N/A	public	No	No	Yes	6
CSP18	No	Yes	No	No	No	N/A	public	No	No	Yes	2
CSP19	No	Yes	Yes	Yes	No	IaaS	public	Yes	Yes	Yes	6
CSP20	No	No	No	Yes	No	N/A	public	No	No	Yes	2
Collaboration sub-group											
CSP21	No	No	No	Yes	No	N/A	public	No	No	No	1
CSP22	Yes	Yes	Yes	Yes	Yes	N/A	public	Yes	Yes	Yes	8
CSP23	No	Yes	Yes	Yes	No	N/A	All	Yes	Yes	Yes	6
CSP24	No	Yes	Yes	Yes	Yes	IaaS and PaaS	All	Yes	Yes	Yes	7
CSP25	No	Yes	Yes	Yes	Yes	N/A	Public	Yes	Yes	Yes	7

Figure 5.1: Comparison of 25 Saas Providers taken from Cloudscape

(See Appendix D for the detailed description of each of these transparency features).

The result of this exercise, although far from being authoritative, confirms that the transparency of the supply chain is not standard across industries. In our analysis, CSPs in the online workspace sub-group were found to be the most transparent. With a mean score of *7.2*, the five CSPs showed a clear understanding of their cloud architecture, provided detailed information about their cloud offering and the steps they took in securing customer data. We discovered that SaaS providers who offered IaaS services were also more transparent than regular SaaS vendors. Also, we found that vertical industry-specific CSPs (e.g. Finance/ERP sub-group) concentrated on their product and its functionality and provided little detail on the supply chain and the security of the product. Our analysis of this vertical industry trend is in threefold; First, SaaS providers do not have enough information on how their service is being provided and have completely outsourced technical control of the infrastructure to their IaaS provider. Secondly, CSPs wrongly assume that their customers are not interested in the security and availability of their data. The third is that it might be that they omitted this information from their website, but are willing to share it with prospective customers at any point.

Nevertheless, we agree with Fischer-Hbner et al. [104], on their suggestion that complex supply chain information should be provided in layers, while also arguing that the eight transparency features we identified can be used as a starting point for all CSPs. We believe that this information would not impede the CSPs competitive advantage; neither would it violate their intellectual rights.

5.1.2 Survey on Cloud Risk Assessment Methods

The survey instrument [229] was administered to a convenient sample of cloud stakeholders between March and July 2017. Although, the heterogeneous way in which firms perceive and manage risk and the limited nature of the sample, means that the analysis of the survey at this stage is only descriptive. Nevertheless, it does provide some insight into the range of risk assessment approaches taken by firms.

After careful analysis of the survey data, a total of sixty-two (62) respondents completed the questionnaire. The analysis of the data confirmed there was no missing information in these responses, as the Boston Online Survey (BOS) tool was designed not to proceed to the next page in cases where mandatory questions were left unanswered. The data that makes up the final dataset in this analysis is made up of fully completed forms. The frequency table -Table 5.1 shows a summary of the demography.

Having established the quality of the participants, we begin our analysis with the response of the cloud providers, followed by that of cloud customers and conclude with the analysis of the general questions posed to all respondents.

Table 5.1: Relevant demographic and cloud computing data from respondents (N = 62)

Demographics		Frequency	%
Principal Industry	Manufacturing	1	1.61%
	Transportation	2	3.23%
	Government	3	4.84%
	Education / Research	4	6.45%
	Other (Media, trade, construction)	10	16.13%
	Finance (Banking, Insurance, etc.)	12	19.35%
	Information Technology/ Telecommunications	30	48.39%
Sector	Private	54	87.10%
	Public	8	12.90%
Company size	1 - 9	12	19.35%
	10 - 50	5	8.06%
	51 - 250	6	9.68%
	251 - 500	5	8.06%
	501 - 1000	6	9.68%
	1000+	28	45.16%
Cloud service model	IaaS	28	45.16%
	PaaS	12	19.35%
	SaaS	22	35.48%
Cloud role	Cloud Consumer (CC)	40	64.52%
	Infrastructure Provider (IP)	4	6.45%
	Cloud Service Provider (CSP)	12	19.35%
	Application Service Provider (ASP)	6	9.68%

5.1.2.1 Cloud Providers

A combined total of 22 cloud providers responded to the survey. The service provided by each of the respondents ranged from cloud security, email, monitoring, storage, runtime/API, customer relationship management (CRM) and financial services. When asked if the respondents carried out a comprehensive risk assessment, the majority of the respondents answered yes, except for three participants. Sixteen providers estimated the level of comprehensiveness for their risk assessment to be in the region of 71% to 100%, while four rated themselves between 51-70% and the remaining two were between 20-50%. The response of the participants to why they conducted risk assessment was not surprising, with the assurance of the security triad (confidentiality, integrity, availability) their top priority. Other suggestions, including the identification of weak links in the supply chain, improved decision-making or a better understanding of risk were lower on their priority list. Interestingly, we observed that on average, each of the cloud providers relied on at least eight other suppliers for the delivery of their service.

While considering if the risk assessment process of cloud providers took into account sup-

ply chain risks, their response showed that 18 of the 22 cloud providers somewhat considered their supply chain risks with varying degrees, while four did not consider supply chain risks at all. With the majority of the responses being positive, this feedback moderately negates their response to the reasons for carrying out a risk assessment, where its use for monitoring weak links in the supply chain had a low response rate. However, in answer to the question of transparency with customers about their dependence on external providers, all but four cloud provider respondents reported that they were transparent. Also on the subject of the transparency of supply chain and its impact on risk assessment, the providers corroborated the results of our earlier research, acknowledging many of the identified transparency features [11] as essential components of a comprehensive risk assessment.

With regards to their risk assessment process, ten cloud providers attested to carrying out a continuous risk assessment of their cloud service, two (monthly), while four each (quarterly and yearly) and the last two only after a security incident. According to Boyens et al. [48], the dynamic nature of the cloud calls for a continuous risk assessment because while the current 'check-box' type risk evaluation system is sufficient for regulatory compliance or adherence to standards, it is inadequate for the accelerated growth of cloud computing [148]. With regards to risk analysis methodology, 17 cloud providers indicated that they used both qualitative and quantitative methods, while five others opted for the qualitative approach. The follow-on question which asked for the specific risk assessment method highlighted the widespread use of qualitative methods, including weighted scoring and risk matrices, which are considered 'weak' quantitative methods. According to Hubbard and Seiersen [143], one of the errors of assessing risk using a risk matrix is that of range compression, where a higher risk cell could contain a lower risk in comparison to another in a lower risk cell.

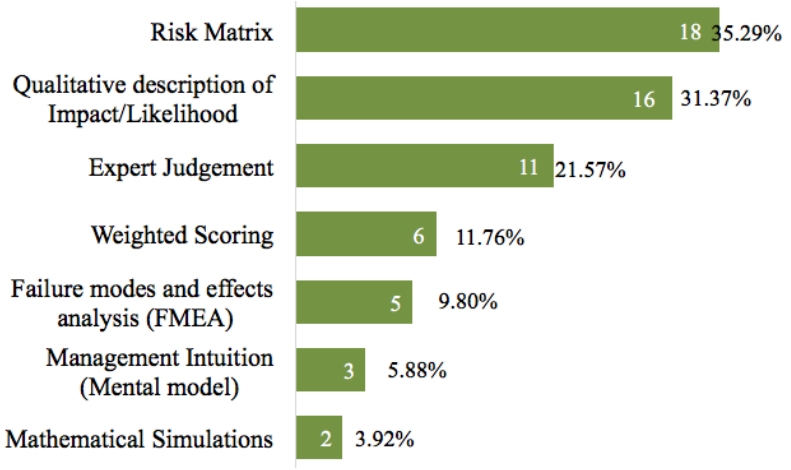


Figure 5.2: Risk assessment methods most commonly used within provider organisations

As Figure 5.2 indicates, the quantitative risk assessment methodologies are not standard within the cloud industry, despite their obvious benefits, including their ability to

maintain internal and external consistency with the meanings and proportionality of the values used for risk estimation. We made this observation also as part of our literature review, so to further establish our findings, we asked cloud providers how the value of risk was expressed within their organisation. Sixteen of those surveyed responded that they used impact/likelihood rating, nine represented risk using its monetary value, five used probability distributions and three expressed risk value using time. In [112], Freund and Jones described one of the advantages of using quantitative over qualitative methods to be its ability to decompose the relevant risk loss scenarios. Such rigour does not seem to apply to the subjective selection of impact and likelihood ratings, further disqualifying the application of qualitative risk assessment in assessing the risk of the cloud supply chain.

5.1.2.2 Cloud Customers

A total of 40 cloud consumers responded to the survey, each of whom are subscribers of at least one SaaS application. Of the 40 cloud customer respondents, 15 were from SMBs (1-250 employees) and 25 were from larger organisations. On the subject of the comprehensiveness of cloud risk assessment, 34 of the respondents indicated they followed a thorough process. Also, 19 respondents confirmed to accounting for their provider's supply chain risks in their risk assessment, while 15 partially considered their supply chain, leaving six respondents who did not consider supply chain risks. Following careful analysis of the respondents who claimed to account for their providers' supply chain in their risk assessments, 25 of them were consumers of email and productivity tools from cloud giants such as Microsoft and Google. On the face of it, it is possible that these respondents erroneously believe their cloud providers are the only member of their supply chain, which is rarely the case.

On the subject of risk analysis methodology, 19 cloud consumer respondents used both quantitative and qualitative models, while 14 used only qualitative, with the last seven respondents using neither of the methods, preferring to use expert judgements on a 'need to' basis. Similar to cloud providers, the use of risk assessment as a decision-making support tool was common also to cloud consumer organisations, and their most common method was also the qualitative description of impact/likelihood, selected by 34 of the 40 respondents. This method seems to be widespread across the IT industry, together with other techniques such as the risk matrices (28 of 40) and expert judgement (22 of 40), see figure 5.3. None of the consumers surveyed used mathematical simulations, which was not shocking, considering the arguments of Freund and Jones [112] and Power [246], on how the bias of regulatory organisations like the NIST and COSO against quantitative risk assessment, influenced the use of more qualitative assessment methods within the IT industry.

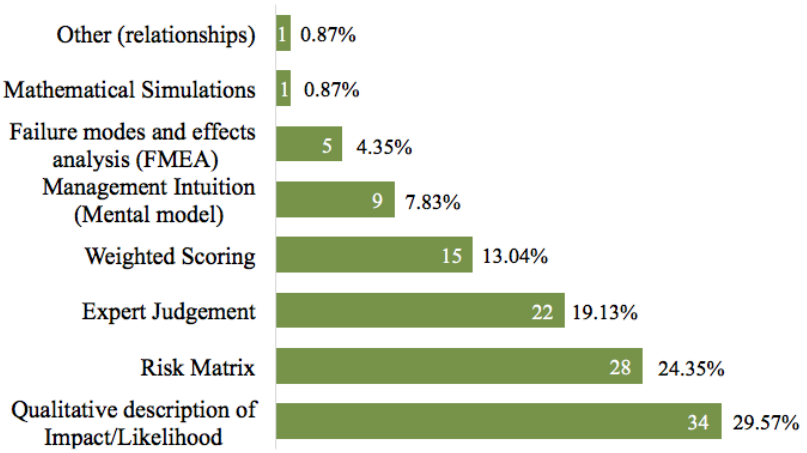


Figure 5.3: Cloud consumers' most commonly used risk assessment method for decision making

5.1.2.3 General Questions

In the concluding section of the survey, the combined group of respondents (62), were presented with a set of general risk and supply chain-related questions. One of the questions required respondents to select what they believe constituted the top four hindrances to a more comprehensive cloud risk assessment, from a list of seven options, as seen in Figure 5.4. While we were not surprised with the choices of the respondents, their emphasis on the need for transparency in cloud computing is in agreement with our earlier work and also the study of [59], which established the extent to which cloud transparency could help to reduce the risk of cloud adoption. Also, we observed that some of the respondents raised the topic of cost and limited training, two factors often cited when SMBs are asked to conduct a quantitative risk assessment [20]. One of the respondents in contributing to the list of hindrances to a comprehensive risk assessment noted the *"lack of awareness amongst suppliers about security risks and how to protect against them"*. The respondent stressed that the *"security standards in the cloud industry were too low"*. Another respondent also identified the hindrance of limited resources, saying *"there is a shortage of qualified experts to perform comprehensive risk assessment"*.

Lastly, seeing that the CSA top 12 treacherous threats [67] was the result of a survey that compiled industry experts opinion on cloud threats, we decided to confirm which of the threats our respondents thought were supply chain-related. Our motivation is to have a validated reference guide for supply chain-related cloud security threats since the CSA survey is widely regarded as the most authoritative and up-to-date cloud survey. As shown in Figure 5.5, the respondents opined that the 12 threats are supply chain-related, with varying level of popularity. This observation follows an earlier established claim by NIST [48], who suggested that the ICT supply chain threat agents are similar to the information

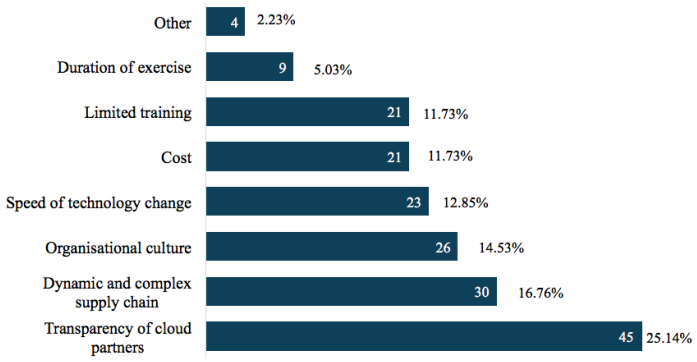


Figure 5.4: Hindrances to a more comprehensive risk assessment

security threats agents, citing insiders and cybercriminals as examples.

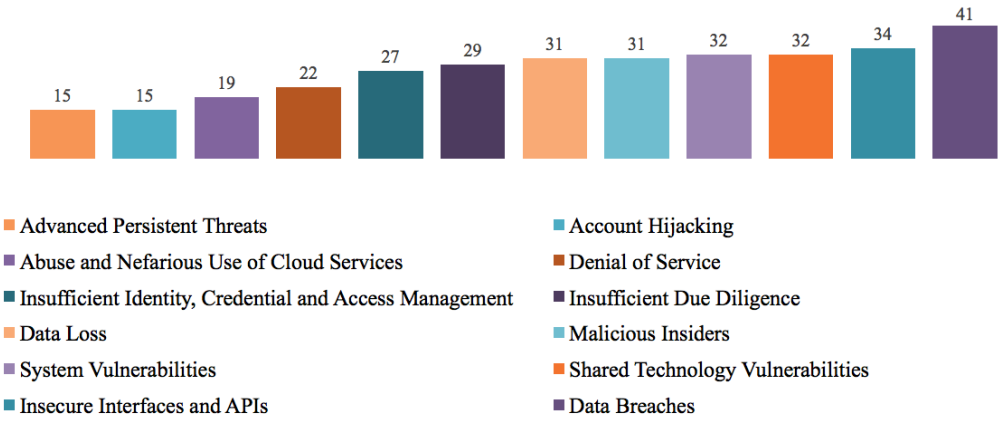


Figure 5.5: CSA's top 12 cloud computing threats that are supply chain related

5.1.2.4 Summary

Together these results provide valuable insights into the level of awareness cloud stakeholders have on supply chain risks and cloud risk assessment. While there seems to be a good awareness of supply chain risks among stakeholders, their approach to assessing the risk cannot be said to be keeping up with the dynamic growth of cloud computing. Despite its exploratory nature, the evidence from this study suggests that the current approach to cloud risk assessment is unable to address the cloud risks. Conducting risk assessments at yearly intervals, give organisations a false sense of security, while the use of qualitative methods for risk assessment is not considered to be rigorous enough to help decompose and model cloud risks appropriately.

Furthermore, there remains the all-important issue of cloud transparency, which as we have seen is a significant component of cloud risk assessment. One concern expressed regarding risk assessment, in general, was the challenge of small enterprises to conduct a cloud risk assessment. These companies who usually do not have a dedicated IT team nor indi-

viduals with the specialised skill for IT risk assessment seem to rely on their cloud provider to take care of their valuable assets. Although the study did not confirm if quantitative risk assessment would provide better results, it did partially substantiate the need for more rigour in cloud risk assessments and provide evidence on how this can be improved with supply chain transparency.

5.1.3 Discussion and Limitations

Despite the exploratory nature of both studies, they provided us with valuable insight into the current trend within the cloud industry, particularly around stakeholder awareness of cloud supply chain risks, their attitude to supply chain transparency and the need to improve the current cloud risk assessment methodologies. Identifying these gaps in the literature, we conducted the first study to explore if the CSP transparency could improve customer risk assessment processes. The second survey, which was a follow-up to the first, sought to verify how stakeholders currently dealt with supply chain risks and the applied assessment methodologies.

These studies contribute to practice and cloud risk assessment research while also providing answers to **RQ1.1 & RQ1.2**. It shows that the delivery of a cloud service is rooted in an inherently complex and dynamically formed cloud provider chain. This complexity of cloud supply chain, made up of sub-tiers of multiple suppliers, increases cloud risk in a way that makes it unlikely to be mitigated by contractual clauses with the CSP. Also, we found out that although there was an incentive for cloud providers to be transparent with their supply chain, not least to gain the trust of their customers, some CSPs refrained from doing this for the sake of maintaining profitability, protecting intellectual property and competitive advantage. Some of the identified reasons for the vague information on supply chains include:

- CSPs are not aware of their supply chain beyond the first tier.
- Cloud customers favour the functionality and cost of a cloud service over its provenance.
- CSPs are uncertain about the quality and quantity of technical and supply chain information to share with their customers.

In response to **RQ1.1**, the result of the study shows that cloud stakeholders' limited visibility or awareness of third party risks, hinders their ability to assess cloud risks adequately. Seeing that risk assessment is a precursor to implementing the appropriate controls to protect valuable assets, the cloud industry stands to benefit from a more transparent approach to cloud provisioning. Therefore, the ability of cloud providers to provide reasonable

visibility of controls and processes both of themselves and their third parties will contribute to the improvement of cloud risk assessment. While not conclusive, this study also makes a significant contribution to addressing: (i) the nature of supply chain information CSPs can share with their customer while still maintaining their competitive advantage; and (ii) the level of information vertical and horizontal market CSPs currently publish on their website.

Furthermore, and in response to **RQ1.2**, the evidence from the cloud risk assessment survey suggests that the current approaches are unable to address the dynamic risks of the cloud, which involves the wider supply chain. Furthermore, with an apparent lack of trust in cloud providers, cloud customers who set out to conduct risk assessments for decision-making, are constrained to carrying out qualitative and subjective assessments due to the limited visibility of security controls. While this study did not confirm if quantitative risk assessment would provide better results, it did partially substantiate the need for more rigour in cloud risk assessments and provide evidence on how this can be improved with supply chain transparency.

However, one of the limitations of these studies is the limited pool of experts who contributed to the studies. This reduces our ability to generalise the results. Also, seeing that most of the stakeholders do not conduct quantitative assessments, or have a good awareness of their supply chain, it was challenging to get exciting feedbacks around the improvements quantitative methods bring into the cloud risk assessment process. Likewise, there is a possibility of participant bias with the risk assessment survey, seeing that we provided the participants with pre-defined options, which were gathered from the literature. While we included the "other" option, to allow them to provide options we might have missed; this was rarely used.

5.2 Delphi Study

In this section, we discuss the results of our Delphi study conducted between January and April 2018, to address the growing need for a consistent approach to assessing the cybersecurity posture of cloud suppliers. The study was conducted over three stages, with 15 cloud experts as our panellist. The result shows that experts achieved consensus on a total of 52 security criteria grouped into nine target security dimensions (see Figure 5.6). These are the security factors that will be used as part of the CSSA tool to rank suppliers based on their security and identify weak links in the supply chain.

Next, we give an overview of each round of the study, followed by the analysis of the results.

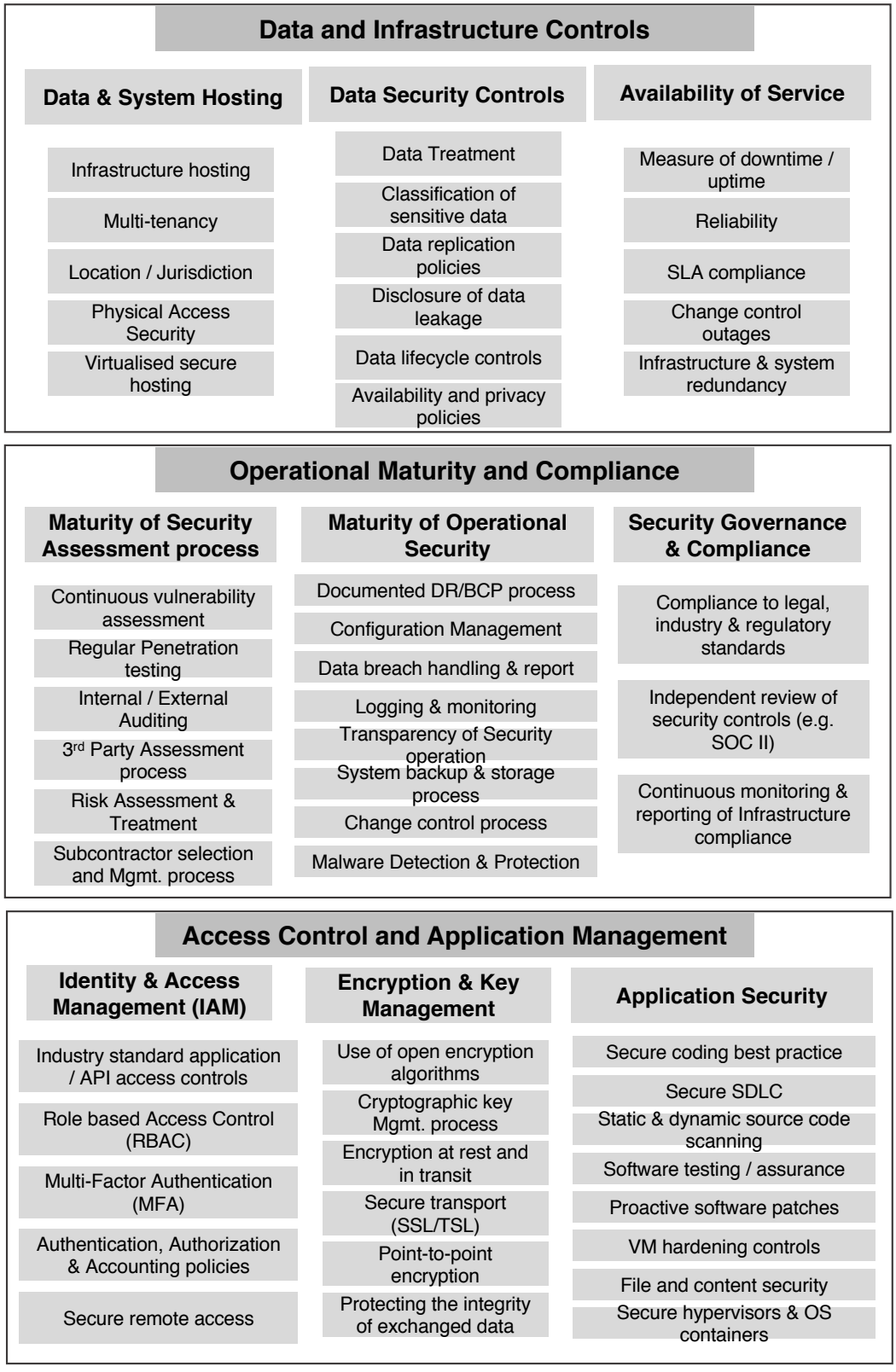


Figure 5.6: Target security dimensions for assessing cloud suppliers - Output of Delphi study

5.2.1 Round One Results

The overall response to the study was positive. We had a 100% response rate with the round one questionnaire. All fifteen (15) respondents who met our eligibility criteria and agreed to take part in the study, completed and returned the questionnaire. The 15-member Delphi study group was made up of thirteen (13) experts who are industry professionals and two (2) from academia (see Figure 5.7).

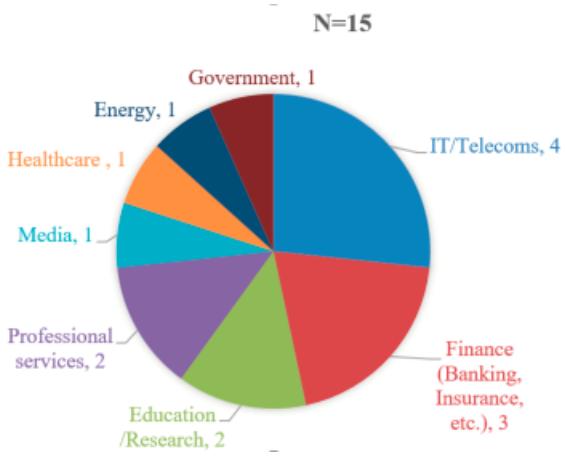


Figure 5.7: Representation of Participant's Industry

The questionnaire presented to the experts in round 1, contained a cloud supply chain scenario of a CRM SaaS provider, who as part of conducting a cloud risk assessment, is carrying out a security rating service (SRS). Each expert was tasked with identifying at least seven (7) criteria he/she will consider in assessing suppliers in such a scenario.

Following the completion of this round, the expert feedbacks were aggregated using an affinity diagram to identify common security factors and their contributing elements. The coding of the expert feedbacks produced a list of 65 criteria, which was grouped into ten (10) security target dimensions. This grouping enumerated the security factors in a logical order and established a consistent and representative naming for each group (see Appendix B for the affinity diagram). The ten security target dimensions are as follows:

1. Availability of Service (AoS)
2. Data & System Hosting (DSH)
3. Cyber Security Awareness /Security Culture (CSA)
4. Data Security Controls (DSC)
5. Maturity of Security Assessment process (MSA)
6. Maturity of Operational Security (MOS)

7. Security Governance and Compliance (SGC)
8. Identity and Access Management (IAM)
9. Encryption & Key Management (EKM)
10. Application Security (AS)

These security factors, together with their contributing elements, provided input for the second round questionnaire that was presented anonymously to the Delphi panel.

5.2.1.1 Round One Analysis

The ten security criteria identified in the round one Delphi study, highlight the details of cloud suppliers' security controls, policies, processes and procedures. Using these criteria, the CSP can apply the CSSA tool in evaluating each supplier's security posture based on a combined implementation, effectiveness and impact metric [127]. Acknowledging that some of the identified factors correspond to security measures included in recognised security standards and control sets such as COBIT v5 [147], ISO/IEC 27001/2 [153] and NIST SP 800-53 [221], we mapped out each security factor to the appropriate standard document (see Appendix B).

5.2.2 Round Two Results

In the second round of the study, 14 of the 15 participants completed and returned their questionnaire, giving us a 93.3% response rate. In this round, we sought to assess the expert's consensus on the identified security factors. Each expert rated the security factors on a scale of 1 (not important) to 10 (very important), according to their experience and preference for such criteria in a supplier assessment exercise. The panel was reminded of the scenario presented to them in round one, to limit their subjectivity and avoid them rating the factors based on anecdotes or recent events.

Figure 5.8 shows the distribution of expert's rating in the second round. Applying our indicator of consensus (IQR ≤ 1 & Mean ≥ 8) to these ratings, a consensus was obtained on four (4) of the ten (10) security target dimensions (see Table 5.2).

With only four security factors achieving consensus in round two of the study, we excluded these factors from the final questionnaire presented to the panel. In round three, we informed the expert panel of the four security factors that achieved consensus and presented them with a prioritised list of the remaining six security factors. For each security factor, the mean score of the expert's response from round two was indicated, together with the expert's scoring.

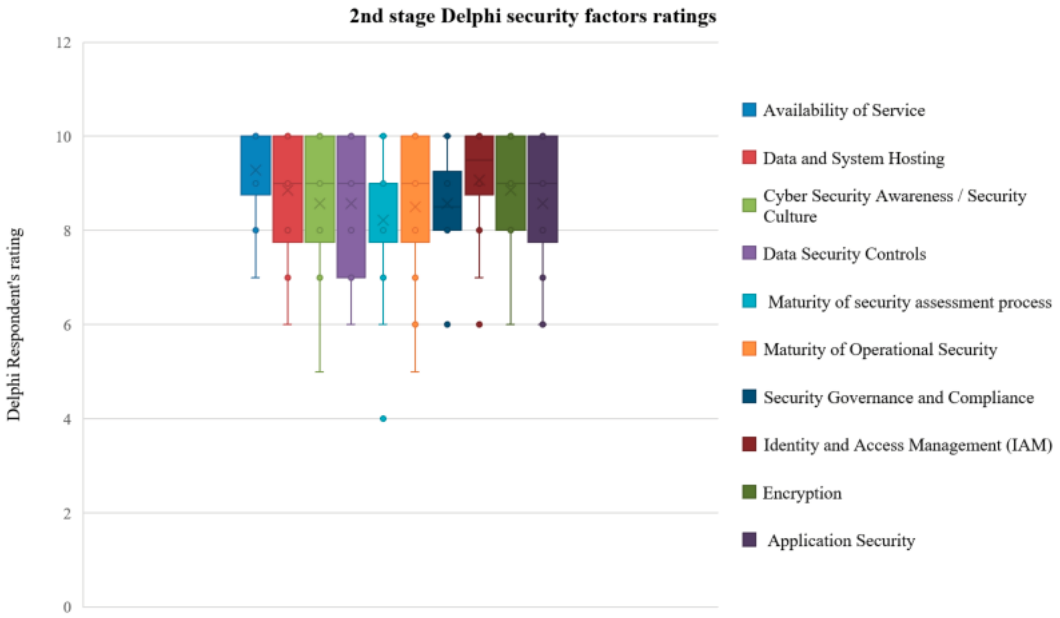


Figure 5.8: Second round Delphi security factors ratings

Table 5.2: Round two assessment of expert consensus on security factors

	Security Factors for Assessing Cloud Suppliers									
Calc.	***AoS***	***DSH***	***CSA***	***DSC***	***MSA***	***MOS***	***SGC***	***IDM***	***EKM***	***AS***
Mean	**9.29**	8.86	8.57	8.57	**8.21**	8.50	**8.57**	9.07	8.86	8.57
Q1	9	8.25	8	7.25	8	8	8	**9**	8	8
Median (Q2)	10	9	9	9	9	9	8.5	9.5	9	9
Q3	10	10	9.75	10	9	9.75	9	10	10	10
(IQR)	**1**	1.75	1.75	2.75	**1**	1.75	**1**	**1**	2	2
Consensus?	**Yes**	**No**	**No**	**No**	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**

5.2.2.1 Round Two Analysis

The four security factors (AoS, MSA, SGC and IAM), which obtained an early consensus among the experts did not come as a surprise. These factors, especially service availability, compliance and identity management, are often prioritised among cloud consumers. There are several possible explanations for this result. One is perhaps due to the recent incidents involving leading cloud providers [307], which has brought these factors to the vanguard. Another possible explanation for this is the current buzz in the IT industry whereby organisations who are preparing for the new EU General Data Protection Regulation (GDPR), are reminded of the need for their process and policy to be compliant, including those of their suppliers [251]. Cloud SLA now demand that suppliers go beyond highlighting the typical availability of service, to translating the actual security controls implemented to assure this availability and the security assessment process that supports its continuous compliance. Availability of service unsurprisingly had the highest mean score (9.29) of all the security

factors considered in round two. Irrespective of the service model, CSPs are required to ensure basic service availability and security [267].

Identity and Access Management, which enable CSPs and consumers to share data across disparate systems and trust boundaries, is another critical factor that was identified. The CSP is required to assess the implementation of controls such as multi-factor authentication (MFA), separation of duties, role-based access control (RBAC) and the use of open standards in application access control systems during supplier selection and these criteria should be monitored for continuous compliance. Furthermore, the need to assess the maturity of the supplier's security assessment process goes beyond evaluating compliance and benefits the CSP in three ways. First, it gives an impression of how suppliers identify and handle internal and supply chain risks, secondly, it helps to evaluate the security culture within the supplier organisation [72], and lastly, it measures the readiness of a supplier to handle a targeted attack or disruption. A supplier who undertakes regular vulnerability assessment and penetration testing of their system, and demands the same from their direct suppliers, will have better visibility of vulnerabilities in their supply chain and will be better prepared to mitigate them, positively impacting the cloud service.

5.2.3 Round Three Results

Table 5.3 shows the results of the third round expert's rating of the security factors and consensus calculation. Thirteen of the fourteen experts who were sent the questionnaire in round three, completed and returned it, giving us a response rate of 86.7% from round one to three.

Here we can see that five of the six security factors presented to the expert's achieved consensus. One unanticipated finding was that the CSA security factor did not reach consensus among the experts. While we felt this was inaccurate, seeing the role cybersecurity awareness plays in an organisation, we have to agree with the collective judgement of our expert panel. Cybersecurity awareness was recently rated in the top three (3) challenges facing IT security professionals in 2017 [308].

One of the experts who had a low rating for cybersecurity awareness mentioned how he could still *use the services of a supplier, even when the supplier did not have adequate staff background checking procedure, or an established security function.* This position perhaps may be explained by the fact that the panellist runs a cloud start-up company who might not be able to meet a similar requirement. Another expert stated that he *could not see how best to rate a supplier's security awareness training program or their information security policy during a CSP's risk assessment.* He maintained that he did not understand how cybersecurity awareness ended up being rated the same or even higher than some of the other security factors. Security awareness training improves response to social engineering

Table 5.3: Round three assessment of expert consensus on security factors

	Security Factors for Assessing Cloud Suppliers					
Respon-dents	***DSH***	***CSA***	***DSC***	***MOS***	***EKM***	***AS***
EXP1	10	8	9	8	9	8
EXP2	10	10	8	10	10	8
EXP3	9	9	9	9	9	9
EXP4	9	9	9	10	10	9
EXP5	9	9	10	9	10	8
EXP6	8	8	8	9	10	9
EXP7	10	7	10	7	8	6
EXP9	9	8	8	8	9	8
EXP10	8	7	9	8	9	7
EXP11	10	10	10	10	9	10
EXP12	9	7	9	9	9	10
EXP13	10	8	8	8	8	8
EXP14	8	7	8	8	9	9
Calculation of Consensus Criteria (IQR<=1)						
Mean	**9.15**	8.23	**8.85**	**8.69**	**9.15**	**8.38**
Q1	9	7	8	8	9	8
Median (Q2)	9	8	9	9	9	8
Q3	10	9	9	9	10	9
IQR	1	2	1	1	1	1
Consen-sus?	**Yes**	**No**	**Yes**	**Yes**	**Yes**	**Yes**

attack [316], and having an established security function has its operational and strategic advantages, but a possible reason for this lack of consensus among experts is that according to Osborn & Simpson [232], the level of security awareness in small organisations has not resulted in mitigated risks. SMBs, which make up a large chunk of the cloud supply chain, cannot afford to have an established security function, and this sometimes hurts their security.

5.2.3.1 Round Three Analysis

In complying with the aim of this Delphi study, the third-round questionnaire provided the panel members with an opportunity to revise their rankings or specify their reasons for remaining outside the consensus [141]. As shown in Table 5.3, the five security factors that achieved consensus are Data and System Hosting, Data Security Controls, Maturity of Operational Security, Encryption and Key Management and Application Security. Data security plays a pivotal role in cloud security. The location of data based on jurisdiction puts a restriction on the flow of data and should be assessed. While customers have limited control over how their data is treated in the cloud, they rely on the provider to assure data security, and this involves monitoring the supply chain for potential misuse and holding

suppliers accountable to their data processing rights. CSPs should be assessing suppliers based on their data encryption, data treatment, data replication and general data lifecycle controls.

Key management is another critical issue in cloud infrastructure. The multi-tenant model of public cloud and the virtualisation of cloud services obscure the identification of the physical key storage location. The confidentiality of encryption keys needs to be maintained to enable the authentication, confidentiality and integrity of data transmitted between systems [337]. The maturity of operational security is another area that is integral to cloud security and will become more prominent post-GDPR, seeing that there is a requirement for organisations to report breaches within 72hrs. Cloud suppliers should have 24x7 monitoring and well-defined processes for diagnosing and resolving incidents and publishing findings and recommendations. These organisations should mature into a stage whereby incident notification, configuration management, system backup, malware detection and change control processes are routine activities.

While all five security factors that achieved consensus in round three of the Delphi study are crucial to the overall security of the supplier and by implication the CSP's cloud service, we are alerted to the problem of lack of transparency in the cloud supply chain [58, 59]. This lack of transparency, particularly of the security controls, makes it difficult to verify some of these controls. Three of the thirteen experts who completed the questionnaire, rated the application security (AS) target dimension a score between six (6) and eight (8), and two of them cited their *inability to reliably verify criteria such as secure coding practice and source code scanning* for the low scoring. Other experts who rated it high (10), wondered why it had a low mean score after round two, reminding the researcher of its importance. With the cloud, critical security controls have moved up the stack into the application layers. Therefore, providers and suppliers alike must be able to demonstrate their competence in protecting client data [280]. Application security poses specific challenges to all members of the cloud supply chain, and a top recommendation by the cloud standards customer council is for organisations to apply the same diligence to application security as they do to physical and infrastructure security [98].

5.2.4 Discussion and Limitations

In response to **RQ2**, the results of this Delphi study found objective and actionable security factors that cloud providers can consider when choosing suppliers for the critical elements of their cloud service. The assessment of the security factors, in comparison to the more popular CSA CAIQ [74], cuts through the need for free text explanations and these factors are highly distinguishable and verifiable. This finding is evident in target dimensions such as data security control. The DSC, which measures the level of security control a supplier

has in place for data lifecycle and classification, data replication and privacy, including disclosure policies, is easily verifiable by the CSP either through SLA or using monitoring techniques. This work also complements previous studies by proposing unbiased security criteria that can be used in assessing cloud suppliers, irrespective of their delivery model (i.e. SaaS, PaaS, & IaaS). Unlike studies that have developed cloud provider selection models based on the SMI [4, 117], this work extends the list of applicable security factors based on practical and measurable criteria. It also allows the CSP to compare the security of suppliers on both high and low levels of abstraction.

However, it is worth noting that the Delphi panel did not address all aspects of the cloud supplier security assessment. For instance, the experts did not identify the need to evaluate the financial viability of cloud suppliers, as required under the SOC I compliance regulation [296]. The reason for this is not apparent, but a possible explanation for this might have something to do with how we framed the SaaS scenario or that the experts were more concerned about the provision of a secure cloud service. Another somewhat disappointing outcome of the study is the lack of agreement among the experts on cybersecurity awareness as a security factor for comparing cloud suppliers. Some of the criteria considered under the cybersecurity awareness target factor include the reputation of the provider, industry certifications and staff security awareness training. While it might be somewhat challenging to assess each of the elements of this particular security factor, we argue that a combined rating could be applied. Another security criteria not addressed in this study, but considered a critical component of any cloud service, is the security of the domain name system (DNS) infrastructure. Surprisingly, none of the experts mentioned DNS security, even though it is a known fact that an attack on the DNS would disrupt the operation of the cloud service, as shown in the DDoS attack on Dyn DNS infrastructure in October 2016 [139].

Taken together, the result of this study is positive. While not ruling out the possibility of CSPs coming up with other security criteria more applicable to their service, we maintain this does not threaten the validity of this study. Also, we understand that these findings will be scrutinised due to the contentious nature of cloud security, but we are encouraged by the level of consensus of the group of experts who participated in the Delphi study. Acknowledging that the result is not generalisable to all implementations of the cloud, it is crucial to understand what the study means for future research. The identified security factors highlight areas of cloud security which cloud providers need to be particular about when choosing suppliers or assessing their risk. These security factors can be considered as a primary step towards the standardisation of cloud supplier's security evaluation and the establishment of a standard vocabulary for cloud risk assessment.

5.3 Summary

The results of these studies are two-fold. The surveys and interview around cloud transparency and the inadequacy of existing risk assessment model established the need for researchers to investigate new cloud risk assessment approaches. In complying with that requirement and considering the lack of a structured framework for cloud assessment, we proposed the CSCCRA model. This model combines quantitative risk analysis with supplier security assessment & supply chain mapping, to provide a more iterative, incremental and inclusive approach to cloud risk assessment. Currently, no other study has addressed the effect of supply chain transparency on cloud risk assessment, and we believe our approach will improve the state-of-the-art both in practice and research.

Moreover, the process of assessing cloud risks using our proposed model, require CSPs to understand the vulnerabilities each component supplier introduces to the delivery of the cloud service. This requirement necessitated our polling of cloud experts on security factors for assessing the cybersecurity posture of cloud suppliers. The result of the Delphi study showed that experts achieved consensus on a total of 52 security criteria grouped into nine target security dimensions, which can be used in rating and comparing the security of vendors within a supply chain.

Collectively, the results achieved from these studies promote the need for increased visibility of security controls and transparency in the supply chain. With this, CSPs become aware of their supplier processes and can proactively improve the security of their cloud service. An advantage of our proposed approach to cloud risk assessment is that it not only analyses the cloud supply chain to determine its immediate risks and weaknesses, it also helps with the implementation of a continuous monitoring system for the cloud service. CSPs can compare the rating of cloud suppliers for each completed assessment to monitor improvements in security posture. At this stage of the study, we hope that the structured and systematic approach of our proposed model would aid decision-makers in understanding their current security posture, evaluate their security gaps, increase the assurance of security investments and identify weak spots in the supply chain.

Chapter 6

The CSCCRA Model

The objective of a risk assessment is to understand the existing system and identify risks through analysis of the information/data collected. This process helps organisations to make security decisions consistent with their risk management strategy, despite the level of uncertainty inherent in the evaluation process. This uncertainty constitutes the following considerations: i) ability to forecast future from past events; ii) incomplete knowledge of the threat; iii) undiscovered vulnerabilities in the technology or product; iv) unidentified dependencies [142, 258]. Therefore, in assessing risks, it is practical to implement a risk assessment framework that employs a rigorous process in determining the risk factors and promotes increased objectivity through the use of controlled experimentation.

With the supply chain of cloud applications, particularly SaaS, almost spiralling out of control, CSPs require a framework to verify the risk of their cloud services. Seeing that each member of the supply chain faces an ever-changing list of security threats which could result in the loss of confidentiality, integrity or availability of service, CSPs have gradually become unable to provide the sort of security assurances customers want for their cloud service. Therefore, to assist CSPs with understanding their cloud risks and objectively assessing these risks, we proposed a novel cloud risk assessment framework. The model considers the changing nature of the cloud supply chain and looks to address the gap on cloud supply chain transparency, and how the lack of visibility of supplier's security controls have contributed to the inadequate level of cloud risk assessment. It also aims to present the CSP's cloud risk in a format that is consistent, repeatable, traceable and understandable, one which encourages proactive mitigation of cloud risks.

The CSCCRA model adopts the systems thinking approach to solving complex system problems as suggested by Ghadge et al. [116]. This method requires us to conceptualise and analyse the interdependencies of the cloud service during risk assessment while making use of modelling and simulation techniques to draw the result of the assessment. The model is built out to empower CSPs to make reliable inferences about the risk of their cloud service and the behaviour of their component suppliers, based on a deep understanding of their

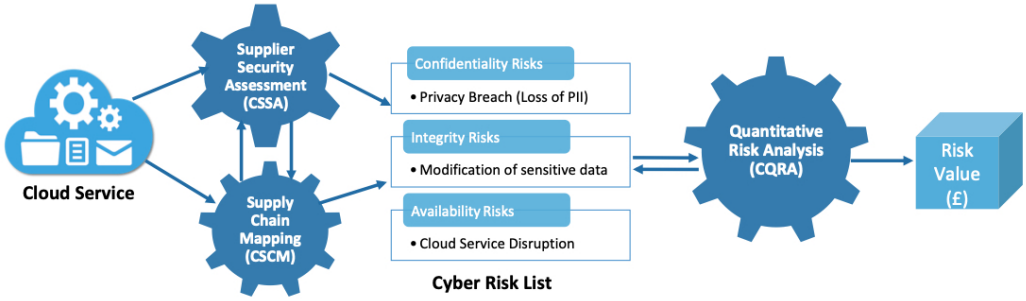


Figure 6.1: The CSCCRA Model

underlying structure. The CSCCRA model builds on existing risk assessment standards and guidance documents such as ISO/IEC 27005:2011, ISO/IEC 31000:2009, NIST 800-30v1 and FAIR risk assessment. The model is made up of three components:

1. Cloud Quantitative Risk Analysis (CQRA)
2. Cloud Supplier Security Assessment (CSSA)
3. Cloud Supply Chain Mapping (CSCM)

The CSCM & CSSA components of the model, help stakeholders to gather initial data on their supply chain and understand the potential risks posed by their suppliers. According to the National Cyber Security Centre's (NCSC) guidance on supply chain security, until an organisation has a clear picture of its supply chain, it will be hard to establish any meaningful control over it [213]. While it is challenging for CSPs to establish control over their suppliers due to the autonomy that drives the cloud supply chain, their use of the CSCCRA model helps them raise security awareness among their suppliers and build security into their contracting process. The process of identifying the components that make up a cloud service, their suppliers, and mapping the supply chain, enables CSPs to understand what needs to be protected and why. Likewise, the process of assessing these suppliers compel the CSP to gather more information on the supplier's security controls, thereby building an understanding of their security posture, and the nature of potential risks masked in the supply chain. Ultimately, the CSCCRA approach to risk assessment encourages the improvement of security within the cloud supply chain and builds trust with suppliers.

6.1 CSCM

According to the supply chain management (SCM) risk maturity model [50], the stage 5 (resilient) level of supply chain capability involves having an end-to-end supply chain mapping across critical products, and a comprehensive and integrated process for conducting

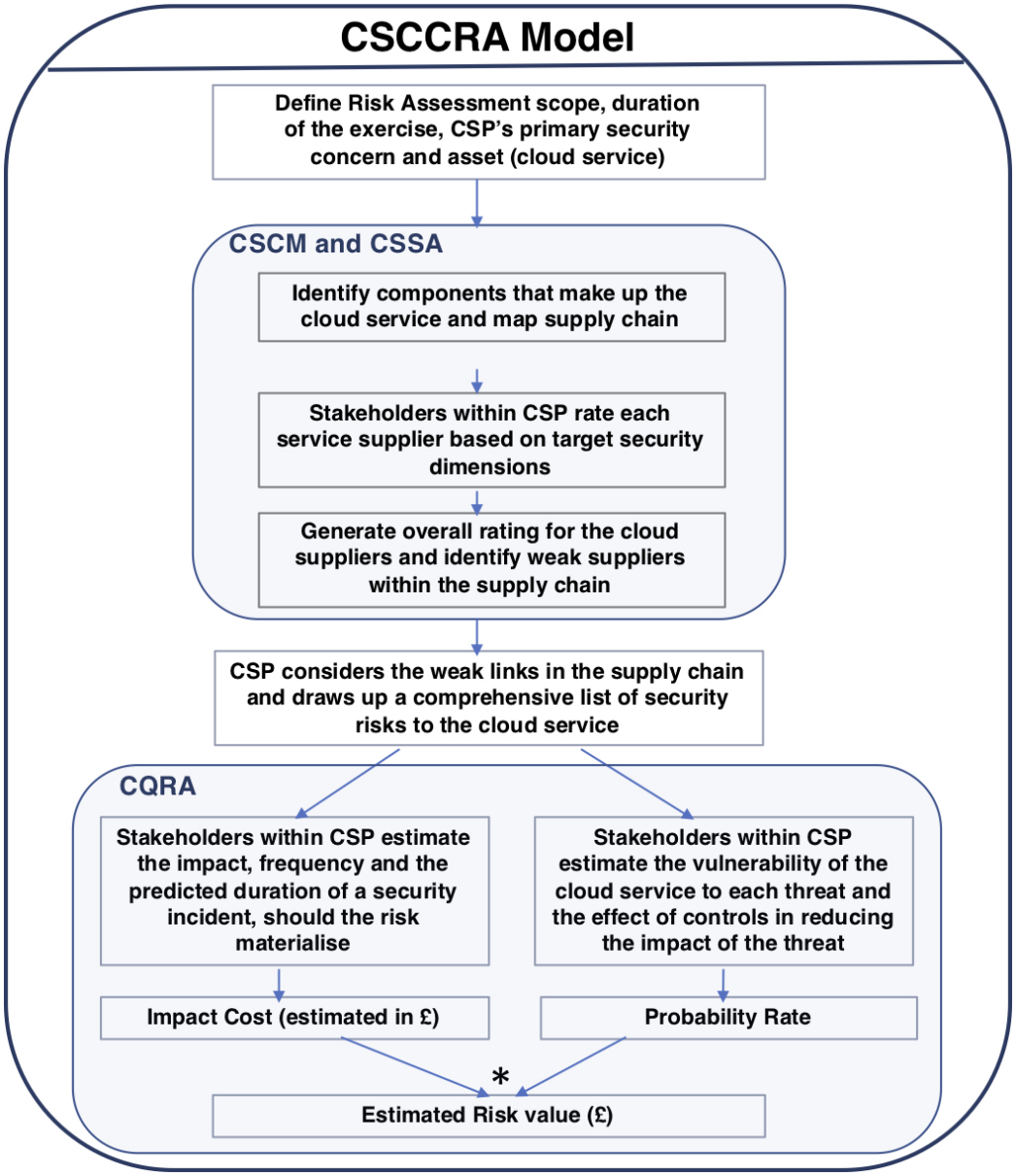


Figure 6.2: Illustration of CSCCRA risk assessment process

the risk assessment. Mapping the supply chain enables focal organisations to recognise the risk in critical but lower-tier suppliers and assess the impact of these suppliers on their service. It establishes a consistent approach to identifying risks by creating visibility and encourages proactive mitigation of security risks across the supply chain. While in some cases finding the initial information might be labour-intensive, time-consuming and complex, SCM encourages providers to work collaboratively to share information, seeing that everyone benefits from the process.

Our supply chain mapping module implies that the ontology of a supply chain structure involves the use of link and nodes. While there is a plethora of commercial and open-source software for supply chain mapping, we have designed and implemented the CSCM

tool using the Neo4j [214], a free-to-download graphing database application. Robinson & Webber [255] define a graph as a collection of vertices (nodes) and edges (relationships). They are a network of related data. The use of a graph database was informed by their performance, agility, flexibility and the level of their connectedness which is in-built, in comparison to other relational databases and NoSQL data stores where developers are required to implement more data processing in the application layer [255]. We live in a connected and dynamic world and storing connected data in recent times can be a challenge. Seeing that the cloud is made up of a complex and interconnected supply chain, representing this level of connectedness in a relational database requires a large number of data joins, which impedes performance. The same also applies to NoSQL databases which lack relationships and are used to store set of disconnected documents, values or columns, so using this to store connected data will require joining aggregates at the application level, which is an expensive process [255].

The CSCM is a tool capable of mapping the supply chain of a cloud service and assisting CSPs in assessing specific risks of the service based on its cybersecurity dependencies, threats and vulnerabilities. It provides the CSP with the ability to recognise suppliers they have relationships with, and the nature of their connection (direct or indirect). The CSCM fits into what is commonly referred to as a "Labelled Property Graph Model", considering that it is made up of nodes, relationships, labels and properties [214, 255]. These primitives are all that is needed to create cloud supply chain models such as the one illustrated in Figure 6.3.

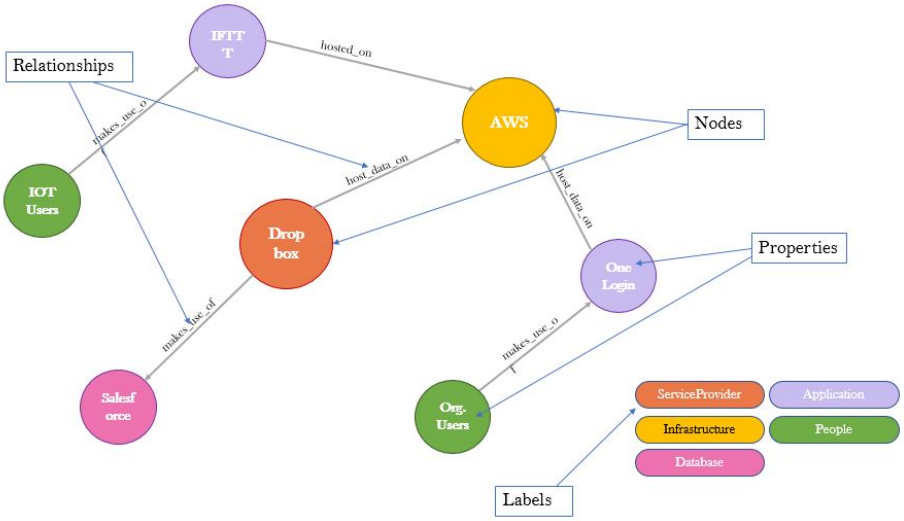


Figure 6.3: Sample Cloud Supply Chain Map

- Nodes - Nodes are the main data elements in a graph model. They contain properties and can have one or more labels which describe their role within the graph. Nodes are

connected to other nodes through relationships. Examples of nodes in a cloud supply chain diagram are application and service providers.

- Relationships - Relationships connect nodes and structure the graph mode. They are directional, and always start and end at a node. Relationships also have properties, and its direction and name add semantic clarity to the structuring of the nodes.

- Labels - Labels are used to group nodes into sets, to indicate the roles they play within the dataset. A node may have multiple labels and labels can be indexed to accelerate finding nodes in the graph.

- Properties - Properties are named values where the name is a string. The ability to add properties to relationships and nodes provides additional metadata for graph algorithms.

Lastly, while we acknowledge the visualisation support provided by the CSCM tool to cloud stakeholders assessing the risk of their cloud service, we also identify its limitations. Seeing that the supply chain is not just a simple linear sequence of connections, but rather an intricate web-like structure which spans several tiers, there is a need to improve on the model so it can generate quantitative measures that characterise the network structure. Such improvement could see the CSCM being used by CSPs to quantify the complexities of their cloud supply chain and understand its transition probabilities.

6.2 CSSA

According to the Institute of Risk Management (IRM) [138], managing the risk of a supply chain can only be as effective as the management of the weakest link. The strength of the cloud supply chain depends on the strength of its weakest member [7]. There is, therefore, a need to gather objective and quantitative measurements of cloud security performance to compare suppliers of a cloud service. These metrics are needed for the continuous security assessment of cloud service, seeing that the traditional one-off cloud risk assessments will not suffice.

The CSSA tool is a novel addition to any cloud risk assessment model, and functions as a Security Rating Service (SRS) for the suppliers involved in the delivery of the cloud service. Seeing that the CSCCRA model requires cloud providers to be aware of their supply chain and have sufficient information about the processes and capabilities of their vendors, the CSSA tool addresses the notion of a distorted and incomplete process involved in cloud supplier selection. Being an MCDM tool, the use of CSSA in cloud risk assessment ensures that decision made around cloud risks, follow a formal and rigorous form. Furthermore, Gartner also encourages organisations to adopt SRS as part of their ongoing program for

third-party cyber risk management [227]. The CSSA, when combined with CSCM, is to be used by CSPs in conducting enterprise-wide socio-technical assessments of the cloud services' supply chain. The process of identifying weak links in the supply chain presents CSPs with valuable insight into their supplier security posture and informs their decision on ways to secure and optimise their chain for cloud service delivery. The result of these processes also furnishes the CSP with a knowledge of their security posture and assists them in drawing up a comprehensive list of risks to the cloud service, which can then be evaluated quantitatively.

Similar to how models have been used to predict the financial posture of organisations(*Alman Z-score*), we proposed the CSSA tool, as a decision support model based on a statistical Z-score (*standard score*) to rank cloud suppliers security controls and identify weak links in the cyber supply chain. We achieve this, using predictive security attributes (security factors) which determine the operational efficiency of the suppliers' security controls. The CSSA tool is based on Dawes's Z-score method of unit-weighted regression. The Z-score helps to standardise the supplier security ratings by measuring how many standard deviations a score is above or below the population mean. Our choice of this approach is influenced by the research of Dawes et al. [80], which showed that the unit (equal) weights of variables could yield predictions that correlate highly with optimally weighted composites if the direction (+1 or -1) in which each predictor is related to the criterion is known. Similarly, Dana and Dawes in [78], demonstrate situations where the use of simple unit weights in predictive models outperform regression coefficients like ordinary least squares, especially when the sample size is small. The Dawes model of unit-weighted regression is therefore optimal for the development of the CSSA tool, because of the positive influence of security factors on the operational efficiency of the supplier's security and the limited sample size made up of suppliers of a CSP.

The CSSA allows the CSP to assess the cybersecurity posture and compare the security of their suppliers on both high and low levels of abstraction. Using the CSSA tool, the CSP evaluates each supplier's security posture based on a combined implementation, effectiveness and impact metric. The tool presents CSPs with a consistent approach to assessing and comparing cloud suppliers based on nine (9) security target dimensions which were achieved through a Delphi study. The stakeholders then score each component supplier based on the nine dimensions on a scale of 1 (least secure) to 10 (most secure). This process assists CSPs in the identification of weak suppliers readily susceptible to cyber-attack or those with a high risk of failure. Likewise, as a decision support aid, the CSSA tool helps to improve not just the accuracy of expert decisions, but also the transparency, consistency, adaptability, accuracy, consistency and speed of the process. Improving the risk assessment process with

the identification of potential weak spots in the supply chain also helps to capture the vulnerabilities of the cloud service and promote proactive mitigation of risks.

CSP's list of suppliers	Availability of Service (AoS)	Data & System Hosting (DSH)	Data Security Controls (DSC)	Maturity of Security Assessment process (MSA)	Maturity of Operational Security (MOS)	Security Governance and Compliance (SGC)	Identity & Access Management (IAM)	Encryption & Key Management (EKM)	Application Security (AS)	Weighted z-scores ====>>	z-score (AoS)	z-score (DSH)	z-score (DSC)	z-score (MSA)	z-score (MOS)	z-score (SGC)	z-score (IAM)	z-score (EKM)	z-score (AS)	
PaaS-A Hosting	8	8	9	9	9	8	8	9	9		-1.10	-0.35	-1.23	-0.96	-0.64	-0.45	0.67	-0.45	-0.96	-0.61
Identity CSP	7	9	8	8	8	8	10	9	8		0.73	-1.23	-0.35	0.24	-0.24	-0.45	-1.57	-0.45	0.24	-0.34
Billing CSP	8	7	8	9	9	6	8	8	9		-1.10	0.53	-0.35	-0.96	-0.64	1.04	0.67	1.79	-0.96	0.00
Custom API CSP	7	6	7	7	8	6	8	9	7		0.73	1.40	0.53	1.43	-0.24	1.04	0.67	-0.45	1.43	0.73
Database CSP	7	8	6	8	3	9	9	9	8		0.73	-0.35	1.40	0.24	1.75	-1.19	-0.45	-0.45	0.24	0.21

Figure 6.4: Cloud Supplier Security Assessment of a Sample Cloud Application

As shown in Figure 6.4, the cloud service is broken down into its individual components based on suppliers, and each supplier is scored on nine security dimensions. The score is then standardised using a Z-score (Z_i) (see equation 6.1), where σ is the standard deviation, y_i is the supplier score and y is the mean of the population. The combined Z-score (see equation 6.2) for a supplier, shown in the last column of Figure 6.4, is a summation of the suppliers' Z-score for each of the nine security dimensions. The use of colour and values are considered as suitable methods for communicating information in a visual framework [123]. The colour in each of the cells in the last column of Figure 6.4, conveys the degree of risk that particular component has, comparative to the rest of the chain. A green cell has the best risk score (least risky), followed by yellow and then red.

$$Z_i = \frac{(y_i - y)}{\sigma} \tag{6.1}$$

$$CZ\text{-}score = \sum_{i=1}^{9} Z_i \tag{6.2}$$

6.3 CQRA

The CQRA makes use of reasoned estimates of security risk factors made by an expert team of stakeholders who have been appropriately calibrated and have a good understanding of the cloud service. To avoid cloud risk assessment being classed as mere speculation or opinion of risk assessors, and moving it into the realm of knowledge, based on informed opinion, making up for the lack of empirical evidence, the CQRA makes use of calibrated assessors, who can make reasonable estimates. According to Clemen & Winkler [65], an expert is empirically calibrated if, upon examining the events for which the expert estimated a "y percent" chance of occurrence, it turns out that "y percent" actually occurred. The data provided by these experts are combined using a stochastic modelling tool (Monte Carlo) to arrive at a realistic risk cost. The role of experts is vital in this process because their

judgements provide valuable information, given the limited availability of "hard data" on security risks and the inherent uncertainties associated with risk analysis [65]. Seeing that we decompose each risk scenarios into its relevant factors (probability, impact, frequency), we request each calibrated expert taking part in the risk assessment exercise, to make independent estimations of the risk factors. The uncertainties in the experts' estimates are presented as a probability distribution, including a Lower Bound (LB), Most Likely (ML) and an Upper Bound (UB), made to a 90% confidence interval (CI). A 90% CI, in our opinion, is good enough, considering the many unknowns in the cloud supply chain.

Estimating these risk factors are also appropriate for our model, seeing that our goal is to reduce and not eliminate uncertainty through the application of measurements. This approach complies with Hubbard's definition of observation, where he says observations are targeted at *quantitatively reducing uncertainty* [143]. While many risk assessment models ignore uncertainty and its associated risk to simplify their decision-making, we have explicitly considered uncertainty and made it an integral part of our model. According to Daradkeh et al. [79], the presence of uncertainty in the values of input variables implies that there are many possible values for each variable. Performing our risk analysis with Monte Carlo helps to build models of possible risk results, as it substitutes a probability distribution for the risk factors whose estimation has some degree of inherent uncertainty. It calculates the risk result over a specific number of iterations (e.g. thousands or tens of thousands), each time using a different set of random values from the probability functions and at the end producing a distribution of possible risk values for a particular risk item [234].

To implement the CQRA tool for analysing cloud risks, we used the @RISK Monte Carlo Simulation Engine by Palisade [235], which is an add-in to Microsoft Excel. Using the tool, experts' estimates of the probability of risk event occurrence and impact cost, are represented by a Program Evaluation Review Technique (PERT) continuous probability distribution, highlighting the minimum, maximum and most likely values. Our choice of PERT is based on studies that have shown that in situations where there is a lack of real data, it is safe enough to assume that the variable of interest follows a normal distribution [112, 161]. Likewise, we adopted the Poisson distribution for the attack frequency, since this distribution expresses the probability of a given number of events occurring within a fixed time, with a known average rate, where the occurrence of events are independent of one another [175]. The Monte Carlo simulation allows us to account for the expert's uncertainty about their estimation, representing the values as a probability distribution. Being able to present experts' combined risk values using the 5% percentile, Mean and 95% percentile, also allows the experts to consider best and worst-case scenarios while determining the value of the risk, which is most likely going to be around the mean/median mark.

6.3.1 Combining Expert Estimates

Figure 6.5 shows the steps taken by the CQRA to combine experts' opinion on security risk factors using Monte Carlo simulation engine. Ideally, we expect at least three stakeholders to participate in each cloud risk assessment exercise, which gives a good base of information, fosters productive analysis and allows for proper calibration of estimated values. Combining these experts' probability distributions, therefore, summarises the accumulated information and enables the risk assessor to present condensed information to decision-makers [65]. While some might see our consultation with multiple experts as a subjective version of increasing sample size, we adopted the probabilistic risk analysis (PRA) approach developed by academic scholar, Norman C. Rasmussen [249], as a way of increasing our information base and resolving any conflicting information or opinions among experts.

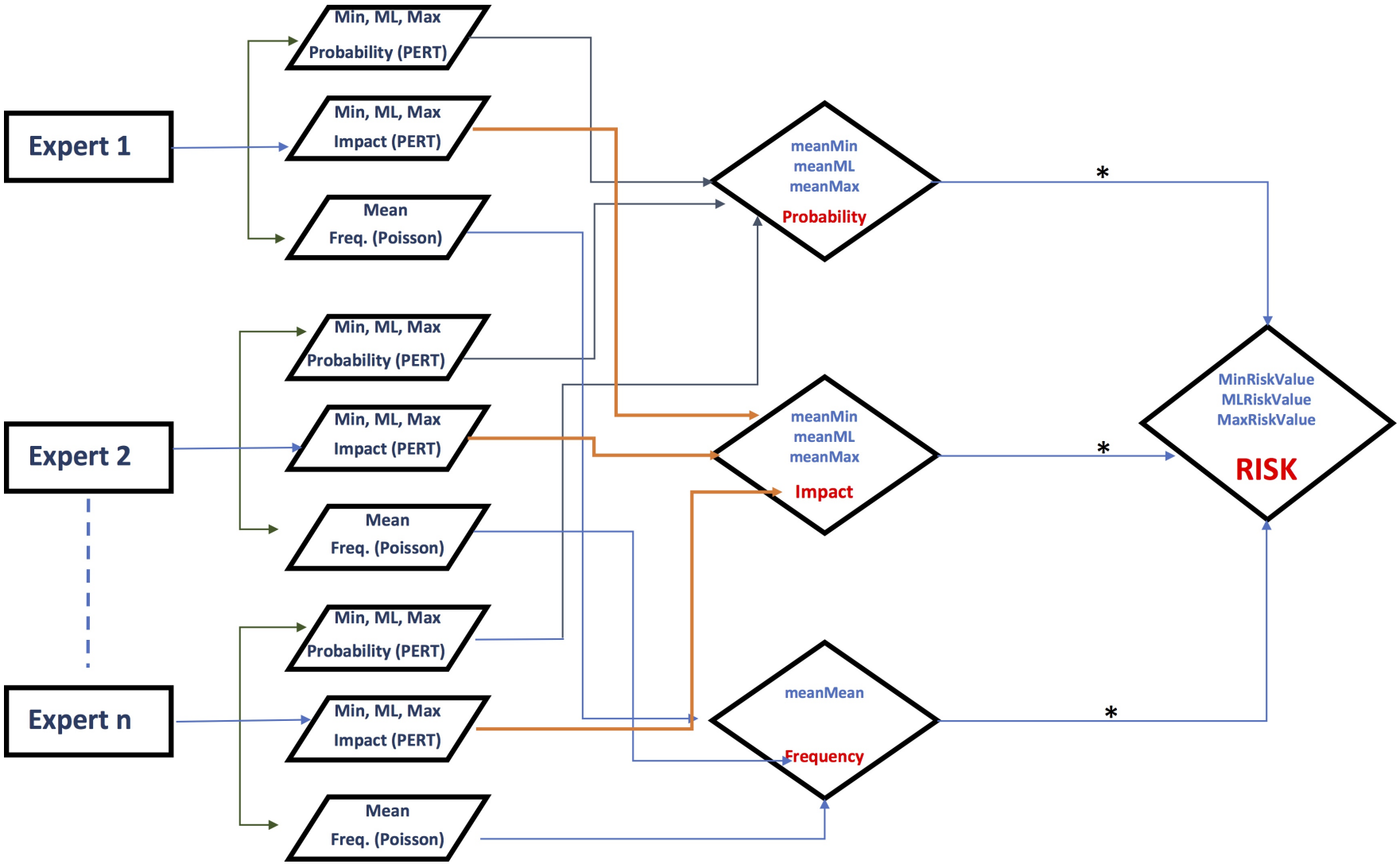


Figure 6.5: Schematic overview of Monte Carlo Expert estimation and Risk calculation

While there are different procedures for combining probability distributions, including mathematical aggregation methods and behavioural approaches [65], our model adopts the mathematical aggregation method based on a *weighted linear average*. This approach, which is also known as the *linear opinion pool*, dates back to Laplace and is a weighted linear combination of the experts' probabilities, where the weights Wi are non-negative and sum to one [65, 88]. The weight assigned to each expert, reflects their competence, or in our case, the specificity of their role, ensuring that the competent experts have a more significant influence on the collective opinion. We considered other approaches including taking the weighted average of the distributions, but this would have caused extreme expert opinions to be under-represented, i.e."*flaw of averages*". Seeing that our model makes use of both the Poisson and PERT probability distribution, we can combine them using the linear opinion pool, because they are mainly unimodal and roughly symmetric. Likewise, empirical results from various studies have shown that simpler aggregation methods outperform the more complex method [65].

We will now describe in detail the CQRA process of combining experts' estimates and how we arrive at the risk value for each scenario. For further details on the risk value calculation, please see Appendix F, where we provided pseudocode for the calculations carried out in the model.

Table 6.1: Expert Opinion Weightings

Contributor	**Weight**	**Sample**
Expert_1	4	0.4
Expert_2	3	0.3
Expert_3	3	0.3
Total	**10**	**1**

Table 6.2: Experts' Estimation of Impact, Probability and Frequency of Risk

Contributor	Risk Factors	Distribution	LB	ML	UB
Expert_1	Probability of risk occurrence without controls (%)	PERT	2	5	10
	Probability of risk occurrence with controls (%)	PERT	1	3	5
	Impact Cost (£)	PERT	2,000	3,000	5,000
			Average Rate		
	Frequency (/yr)	Poisson	1		
Expert_2	Probability of risk occurrence without controls (%)	PERT	10	25	60
	Probability of risk occurrence with controls (%)	PERT	1	5	15
	Impact Cost (£)	PERT	500	1,000	10,000
			Average Rate		
	Frequency (/yr)	Poisson	5		
Expert_3	Probability of risk occurrence without controls (%)	PERT	1	5	10
	Probability of risk occurrence with controls (%)	PERT	1	3	5
	Impact Cost (£)	PERT	3,000	5,000	9,000
			Average Rate		
	Frequency (/yr)	Poisson	0.2		

Using Tables 6.1, 6.2, & 6.3, we describe the process by which three experts provide probability, impact cost, and frequency estimates for a fictional risk event scenario. The risk event involves a service outage caused by a DDoS attack. The experts give two probability estimates: the first is based on a situation where there are existing controls (PwCE), and the other when there are no security controls (PwoCE). We use the experts estimates (see Table 6.2), their weightings (see Table 6.1), and the aggregation of the values (see Table 6.3), to arrive at a distribution of possible risk values. For every risk factor estimate provided by the experts, the CQRA generates a PERT or Poisson distribution to represent the expert's opinion, after which the tool randomly selects a value from each trial to calculate the risk value. The RiskDiscrete function is used to combine the distributions as it samples the expert's estimates according to their weights.

Table 6.3: Combining Experts' Risk Factor Estimation based on Weightings

%Sample	PwoCE (%)	PwCE (%)	Impact Cost(£)	Frequency
0.4	5.33	3.34	3,167	1
0.3	2.83	2.12	2,416	5
0.3	5.16	3.04	5333	0
Combined Expert Opinion (Randomised)				
1.	5.33	3.01	2,417	5
2.	3.95	2.90	5,333	0
3.	3.52	2.32	4,791	1
4.	7.46	4.37	3,313	1
n iterations	4.92	3.78	2,907	2

The CQRA tool, therefore, applies the combined probability distribution of experts' estimates to equations 6.2 & 6.3, in calculating the risk value for both when controls are in place and otherwise (see Table 6.4). The final risk value is presented as a pound (£) value with three estimates (lower bound, mean value and upper bound). Moreover, the choice of which risk value is acceptable to the decision-makers depends on their risk appetite. In this example, we consider the nature of the threat and vulnerability of the application, and based on this analysis we arrive at a most likely (ML) risk value which sits around the 85% percentile of the ERV_WoC distribution.

$$ERV\_WC = Impact * Freq * PwCE \tag{6.3}$$

$$ERV\_WoC = Impact * Freq * PwoCE \tag{6.4}$$

Both Figures 6.6 & 6.7 are a graphical representation of the risk value distribution for situation when security controls are in place and otherwise. The simulation was carried out using @RISK Monte Carlo Simulation tool, where we ran five (5) simulations of 10,000

Table 6.4: Estimated Risk Value based on Expert's estimation

Output (Estimated Risk Value)	**Without Controls (ERV_WoC)**	**With Controls (ERV_WC)**
5% Percentile (£)	0	0
Mean (£)	880	285
95% Percentile (£)	4,182	1,213
Estimated Risk Value (Most Likely)	**£2,222**	

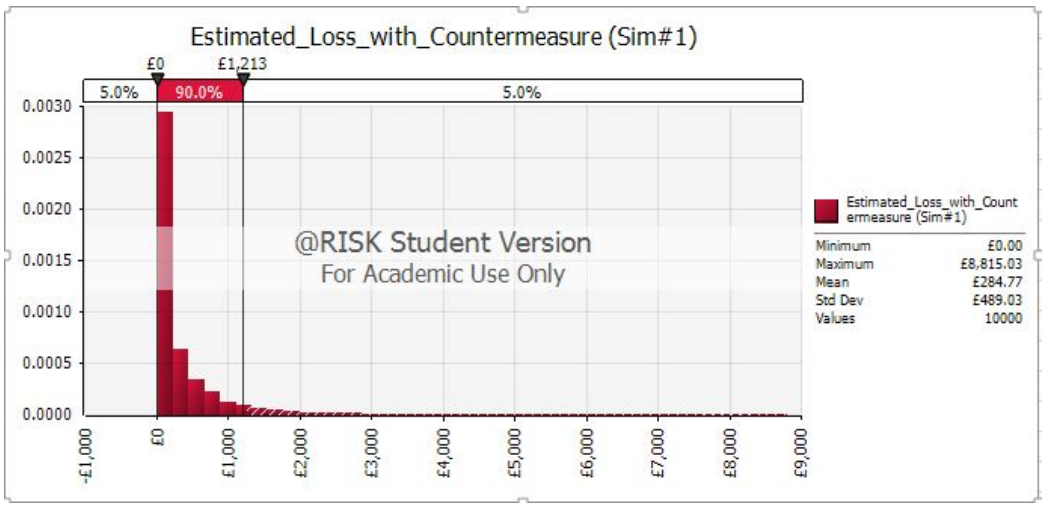


Figure 6.6: Risk value result considering security controls carried out in @RISK simulation engine

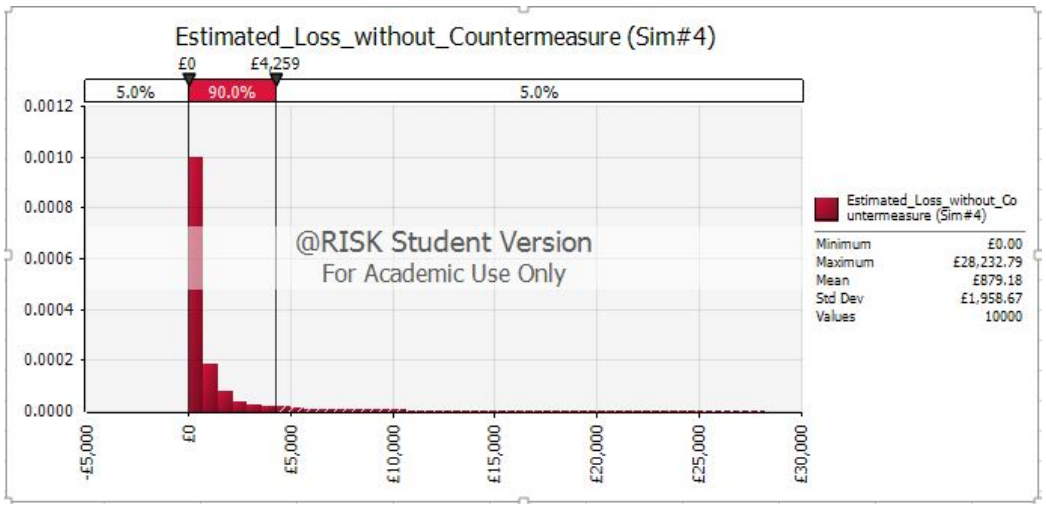


Figure 6.7: Risk value result without considering security controls carried out in @RISK simulation engine

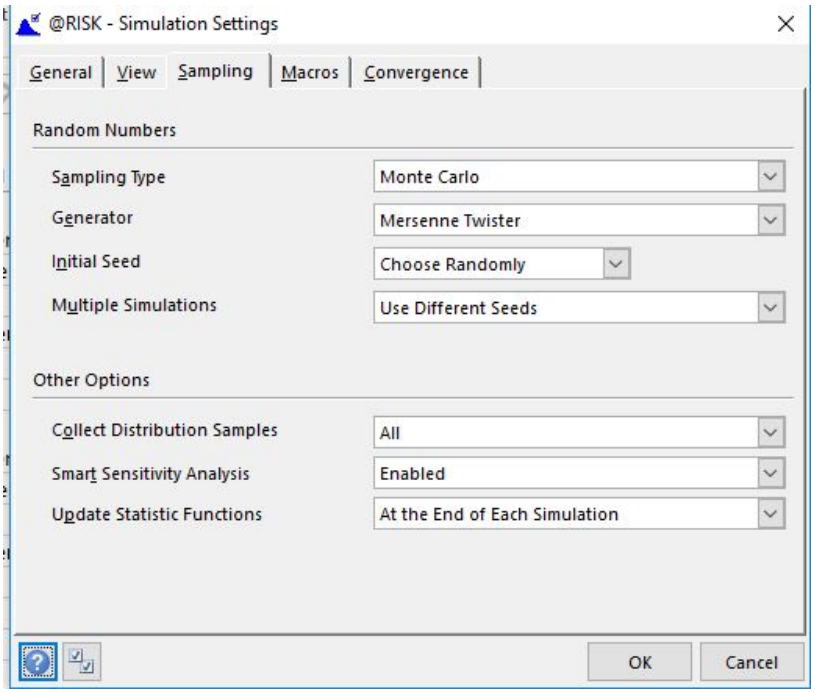


Figure 6.8: The @RISK simulation setting used for the risk value calculation

iterations each (see Figure 6.8 for the @RISK simulation setting).

Collectively, we have shown that the process of combining experts' estimates in risk analysis is valuable for encapsulating the accumulated information around the risk event and yielding objective risk results which provide decision-makers with a clear picture of their risks. We reckon that both normatively and empirically, combining experts judgement improves the quality of probabilities [65]. For more information on the risk analysis steps, see Appendix F.

6.4 Summary

In this section, we proposed CSCCRA as a quantitative risk assessment model which builds on existing risk assessment standards and guidance documents. Its supply chain-inclusive approach addresses some of the transparency gaps identified in existing cloud risk assessment models. The assessment process involves identifying the components of a cloud service and corresponding supplier and presenting this information to stakeholders as a map or data flow diagram. The CSSA component of the model is a supplier rating service, which uses a multi-criteria decision-making method to rank suppliers' cybersecurity posture. The CSSA is designed to bring transparency to the security risk rating of cloud suppliers, provide a quantitative measurement of security performance across the chain, identify the inherent risks and compare suppliers based on their cybersecurity posture. The risk analysis phase allows multiple stakeholders to participate in risk identification, estimation and evaluation

process and presents cloud risk values in monetary terms to promote optimum and effective decision-making.

6.5 Sensitivity Analysis of the CSCCRA model

Following the implementation of the model, we conducted a sensitivity analysis (SA) to find out errors in the model, validate its robustness, identify sensitive or significant variables, and increase our understanding of the relationship between input and output variables. Saltelli et al. [266] defined sensitivity analysis as the study of how the uncertainty in the output of a mathematical model can be attributed to different sources of uncertainty in the model input. Sensitivity analysis identifies the variables that have a significant impact on the model's performance, further reducing the error tolerance within the model. As a decision support tool, simple approaches to SA provide transparency and are easy to understand and communicate.

Seeing that the CSCCRA is a data-driven model that is based on expert input, the sensitivity analysis of the model follows a parametric bootstrap approach [266]. Using Monte Carlo methods for risk analysis requires the sampling of factor values from a distribution, and the independence between the estimated risk factors makes it possible for samples to be taken from the marginal distribution of each factor.

Some of the useful tools for presenting SA results include Scatter plots, Tornado charts and Spider diagrams. Other methods include the use of probabilities, sensitivity indices, graphs and regression analysis [236]. A scatter plot enables the plotting of output variable against individual input variables, following the random sampling of the model over its input distributions. With the scatter plots, the important factor is identified by the existence of "shape" or "patterns' in the points, while a uniform cloud of points is a symptom of a non-influential factor. A sensitivity index is a number calculated by a defined procedure, and it denotes the relative sensitivity of results to different parameters of the model [236].

6.5.1 Experimental Design

In the design of this SA experiment, we aim to find out which cloud risk factor has the most influence on the estimated risk value (output). The input to the model is made up of three risk factors: Probability of risk occurrence, Impact cost and frequency. Expert stakeholders estimate each risk factor based on their understanding of the cloud risk, and experts' estimates are combined to enable the risk assessor to present a single risk value to decision-makers. Although the CSCCRA model does not provide the risk assessor with an optimal strategy for calculating risk value, it simplifies the process by combining different expert estimate to provide a reasonable risk value. That said, with risk value varying with expert inputs and the risk factor estimates largely independent, our modelling approach

only varies one risk factor (impact, probability, frequency) at a time, leaving the others at their estimated values. Our overall procedure is as follows:

1. Tabulate expert risk factor estimations, combined values and risk value calculation.
2. Using spider diagrams and scenario analysis, identify the sensitivity of input variables.
3. Conduct sensitivity analysis using Scatterplots.
4. Identify important parameter(s) that influence risk value.
5. Test alternative assumptions for the value of the input risk factors.
6. Use a different risk scenario to confirm sensitivity analysis result.
7. Summarise the analysis.

As mentioned previously, our sensitivity analysis is based on the assumption that there is no systematic relationship between the risk factors, i.e. the increase in the probability of a risk occurrence does not directly increase or reduce its impact or frequency value. Therefore, we ignore the low risk that any two factors will have a substantial change from base values at the same time. All analysis was conducted using the Palisade @RISK tool, and the results are presented in Appendix F.

6.6 Expert Validation of the CSCCRA model

Risk assessment models should be subject to evaluation and improvement activities to ensure they meet the needs of a myriad of users. The opportunity to face-validate the CSCCRA model with risk experts came when we received an invitation from BCSs' Information Risk Management and Assurance (IRMA) group. The IRMA group invited us to give a presentation on cloud risk assessment and share insights from our research. The talk which we titled "Cyber supply chain risk assessment of cloud services", was given on the 11th of September, 2018, to a group of 25 risk professionals in London, England. We set the tone before the start of the presentation by informing the participants of our plan to face-validate our proposed risk assessment model. We delivered our presentation on assessing cloud supply chain risks, and towards the end of the presentation, we gave the participants an in-depth look into the workings of the CSCCRA model. We demonstrated the applicability of the model using a fictional case study of a SaaS CSP.

Ten risk experts took part in the face-validation of the model. We presented and discussed the various phases of the model with the participants, and gave them room to ask questions and comment on the various stages of the assessment. We simulated the risk

assessment exercise and assessed one of the identified risks, with the experts fully participating in the process. We discussed the pros and cons of the model with the participants and exposed them to the need to apply such an approach to assessing the risks of dynamic and composite services. Next, using a set of questions on a five-point Likert scale, we requested that participants anonymously rate the model on criteria such as its understandability, usefulness, ease-of-use, decision-making ability, transparency and practicality. We also presented them with a free-text for any additional comments such as areas where the model can be improved and its strengths & weaknesses.

The experts evaluated the CSCCRA model based on two aspects: the model's construct and its instruments [265]. The responses of the experts and their ratings of the different components of the CSCCRA model were analysed using the mode average. We considered that a mode value higher than five (5) constituted overall agreement with the assertions made. According to Robertson [254], the mode is an appropriate average for reporting ordinal Likert-scale data. The feedback received from the participants was positive. While many complimented us on giving an excellent presentation and addressing a practical industry need, others confirmed how the research had changed their view of cloud risks. In Figure 6.9, we see that participants strongly agreed or agreed with the majority of our statements regarding the usefulness, practicality, reproducibility and decision-making abilities of the model. However, one of the participants was not convinced about the ease-of-use and reproducibility of the model. In his comment, he said '*"the main next step for the model is the practicalities of using this without it becoming a burden / large upfront exercise".*

Overall, the participants confirmed the usefulness and applicability of the model for assessing cloud provider risks. The evaluation provided us with valuable feedback on the viability of the model and caused us to think through the activities that take place during the assessment. The current CSCCRA process includes some of the suggestions made by the expert review group.

Criteria	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Supply Chain Mapping (CSCM)					
The CSCM tool is a good first step in the risk assessment process	♦ ♦ ♦♦ ♦ ♦♦	♦ ♦ ♦			
Identifying and mapping your cloud supply chain enables you to visualise data flow, and assists in thinking about security (CIA) risks.	♦♦ ♦ ♦♦ ♦ ♦ ♦♦	♦			
Supplier Assessment (CSSA)					
The identified target security factors used in the CSSA tool are appropriate for rating the security of cloud suppliers.	♦♦ ♦ ♦♦	♦♦ ♦ ♦♦			
The result of the CSSA improves your understanding of potential cloud risks.	♦♦ ♦ ♦♦	♦♦ ♦ ♦♦			
Quantitative risk analysis (CQRA)					
The process of estimating the risk factors (impact, probability etc.) helps to limit expert subjectivity.	♦♦ ♦ ♦♦ ♦	♦ ♦ ♦	♦		
The risk formula and resulting risk value is a good representation of cloud risk.	♦♦ ♦ ♦♦	♦ ♦ ♦♦	♦		
Overall CSCCRA model					
Understandability					
The steps of the model are easy to understand	♦ ♦ ♦♦	♦ ♦ ♦♦♦	♦		
Ease of Use					
The model is easy to use	♦ ♦ ♦♦	♦ ♦ ♦♦	♦♦		
Usefulness and Practicality					
The model is useful for assessing cloud risks.	♦♦ ♦ ♦♦ ♦	♦ ♦ ♦	♦		
The model's approach to addressing cloud risk is practical for use in the cloud industry.	♦♦ ♦ ♦♦ ♦ ♦	♦♦			
The result of the risk assessment is reproducible and verifiable.	♦♦ ♦ ♦♦	♦ ♦ ♦♦	♦		
The result of the model helps with decision-making and the implementation of mitigation.	♦ ♦ ♦♦ ♦ ♦♦	♦♦	♦		

Figure 6.9: Expert Validation of the CSCCRA model

6.7 Completeness comparison of the CSSCRA model with established models and standards

Having discussed in section 2.2, three of the existing risk assessment standards and guidance documents referenced in the development of the CSCCRA model, we now look to compare CSCCRA's completeness with that of already established methods. Here, completeness refers to an evaluation of whether the model considers all relevant inputs, includes all necessary tasks and whether the model outputs are linked to concepts of IS risks [204]. While several frameworks could have been selected to conduct this comparison, we chose the Core Unified Risk Framework (CURF) [324]. The framework is proposed as an all-inclusive approach for comparing different risk assessment method [324]. All-inclusive, because the criteria for estimating the completeness of a risk assessment method, organically

grow by adding new issues and tasks from every reviewed method. CURF allows for a detailed qualitative comparison of processes and activities in each RA method and provides a measure of completeness. It is scoped to compare the content of methods to a predefined set of criteria instead of evaluating process tasks or the issue the method is designed to address.

In their study, Wangen et al. [324] applied the framework to assessing 12 formal information system risk assessment (ISRA) methods and found ISO/IEC 27005:2011 to be the most complete approach overall, and both FAIR and ISO/IEC 27005:2011 to be the most complete for risk estimations. In this section, we will be assessing the CSCCRA based on the three main risk assessment processes: risk identification, risk estimation and risk evaluation, and scoring each task identified under the main process. As shown in Table 6.5, we evaluate if each task is **Addressed (XX) = 2**, **Partially Addressed (X) = 1** or **Not Addressed (-) = 0**.

According to Wangen et al.[324], a baseline level of security can be achieved through compliance with standards, legislation and regulations, but to align with industry best practice (cloud in our case) is highly dependent on having a tailored and functional information security risk management (ISRM) processes. Our model helps CSPs to complete two of the most common risk identification activities, i.e. asset identification and evaluation. The unique addition of the CSSA and CSCM pre-assessment steps tailors the model to assess the risk of composite systems. Furthermore, to improve the completeness of our proposed model, we accompanied it with an application software, available to CSPs who are interested in using the model in assessing their cloud service.

1. **Risk Identification:** CSCCRA's risk identification process follows a risk scenario approach, which accounts for the major risk factors that play a part in the risk event. It identifies the asset (cloud service), vulnerability, threat, impact, consequence and existing controls. Its pre-assessment activity leads to risk identification and risk scenario development. It helps to identify situations where an asset could be vulnerable without being threatened or threatened without being vulnerable, or where a vulnerable asset is not critical to the organisation.

2. **Risk Estimation:** The CSCCRA is a quantitative risk assessment model that defines risk as a function of events, consequences, frequency, probability, and their associated uncertainties. It uses the Monte Carlo simulation for the calculation of risk value, accounting for the expert's uncertainty about their estimation and representing risk value as a probability distribution. The model incorporates a control efficiency assessment into the probability of risk event estimations, to provide stakeholders with the strength of their existing controls.

3. **Risk Evaluation:** The final phase of the CSCCRA model is the risk evaluation, where the analysed risks are evaluated and prioritised according to their risk values. Also, during this phase, the risk assessor makes a recommendation to the CSP about the treatment of their top ten risks using security best practices as a guide. This provides the decision-makers with the information they need prioritise and mitigate their risk according to the available resources.

In Table 6.6, we place our self-evaluated CSCCRA scores alongside other established models. In this evaluation, the CSCCRA model had a completeness score of *79* out of a possible total of *102*. The evaluation of the other models was completed in Wangen et al. [324] where more information on the scoring can be found.

Critically looking into the CSCCRA framework and comparing its completeness with other well-established models like ISO/IEC 27005, NIST 800-30, FAIR and ISACA's RiskIT, we see that the CSCCRA has made functional improvements on the existing models. Applying the criteria outlined in the CURF framework shows the CSCCRA model met most of the requirements for each stage of the risk assessment process and can be judged to be the most complete method. Nevertheless, this result must be interpreted with caution because our scoring of the CSCCRA was based on a self-appraisal, and the complete objectivity of the evaluation completed by Wangen et al. [324] cannot be ascertained.

That said, although the performance of the CSCCRA model can be attributed to the fact that the model builds on existing risk assessment standards and guidance documents, the novelty to expand its functional scope to include the supply chain also plays an integral part in its success. The test also shows the extent of the CSCCRA model's granularity as a risk assessment framework and its adaptability to assessing the risks of any other composite system.

6.8 Systematic evaluation of CSCCRA with other conceptual models

In this section, we systematically evaluate three other conceptual models that have been proposed to address cloud service provision risks, comparing them with the CSCCRA model [17]. To determine the most suitable and relevant models for our analysis, we defined a series of search criteria. The first was that the model's approach needed to be relevant to CSP risk assessment; this is to ensure that the identified models address similar challenges with our proposed model. Secondly, it was important that the selected model included information on the parties involved in the development, hosting, management, monitoring or use of the cloud services (i.e. the supply chain). This criterion was necessary to ensure the selected models were inclusive in their assessment of cloud provisioning risks and did

Table 6.5: Scoring CSCCRA's Risk identification, estimation and evaluation process using the CURF framework

Risk Identification	Score	Risk Estimation	Score	Risk Evaluation	Score
Preliminary assessment	XX	Asset identification and evaluation	XX	Risk criteria assessment /revision (RCA)	X
Risk criteria determination	XX	Threat willingness/ Motivation	X	Risk prioritisation/ Evaluation (RPE)	XX
Cloud-specific risk considerations	XX	Threat capability (know how)	X	Risk treatment recommendation (RTR)	XX
Business objective Identification	XX	Threat capacity (Resources)	-		
Key risk indicators	XX	Threat attack duration	-		
Stakeholder identification	XX	Vulnerability assessment	XX		
Stakeholder analysis	XX	Control efficiency assessment	XX		
Asset identification	XX	Subjective Probability Estimate for event	-		
Mapping of personal data	X	Quantitative Probability Estimate for event	XX		
Asset evaluation	XX	Subjective impact estimation	-		
Asset owner and custodian	X	Quantitative impact estimation	XX		
Asset container	XX	Privacy risk estimation	X		
Business process identification	X	Utility and incentive calculation	XX		
Vulnerability identification	XX	Cloud vendor assessment	-		
Vulnerability assessment	X	Opportunity cost	XX		
Threat identification	XX	Level of risk determination	X		
Threat assessment	X	Risk aggregation	XX		
Control identification	XX	*Event,*	XX		
Control assessment	X	*Consequence,*	XX		
Outcome identification	XX	*Uncertainty,*	XX		
Outcome assessment	X	*Probability,*	XX		
Asset,	XX	*Model sensitivity,*	XX		
Vulnerability,	XX	*Knowledge about risk*	X		
Threat,	XX				
Outcome	XX				
Completeness (Total)	**43/50**		**31/46**		**5/6**

Table 6.6: Comparing CSCCRA's Risk identification, estimation and evaluation process with other established models.

	CSCCRA	CRAMM	FAIR	OCTAVE Allegro	ISO 27005	NIST 800-30	RISK IT	Max Score
Risk Identification	43	29	26	32	38	24	29	50
Risk Estimation	31	10	30	14	27	26	22	46
Risk Evaluation	5	4	2	5	3	2	4	6
Completeness Total	**79**	**43**	**58**	**51**	**68**	**52**	**55**	**102**

not just concentrate on the focal CSP. Three of the models listed in Table 3.1 met these criteria and they are QUIRC[271], OPTIMIS [89], & CSPRAM [19].

Next, using examples, we describe the three other conceptual models and compare them with the CSCCRA. For each approach, we consider goals, the risk assessment process, decisions, the scope of the assessment and way in which risk is conceptualised (see Table 6.9).

6.8.1 QUIRC

Saripalli et al. [271] proposed the quantitative risk and impact assessment framework (QUIRC) model for assessing security risks associated with cloud computing platforms based on six key security objectives (SO): confidentiality, integrity, availability, multiparty trust, mutual auditability and usability. The proposed model is based on the premise that most of the typical attack vectors and events, map to one of these six categories. With the model being semi-quantitative, the authors maintain that their approach enables stakeholders to comparatively assess the robustness of different cloud offerings in a defensible manner.

The steps taken to assess cloud risks with QUIRC requires a trained team to perform risk estimations. The risk assessment process is divided into two phases: impact assessment and probability assessment. The impact assessment employs a wide-band Delphi method [189] in collecting external experts' estimate of the impact (I) of a threat to a security objective. This approach is suggested as a scientific method for achieving a consensus among the expert team on the estimate of impact values. Also, due to the lack of historical data on cloud outages, QUIRC relies on security reports (e.g. SANS Institute report [270]) in an attempt to evaluate the probability (P) of threat events.

QUIRC defines risk as a product of the Probability (Pe) of a security compromise, i.e. a threat event, e, occurring, and its potential Impact Ie, where Ie is assigned a value on a numerical scale based on the Federal Information Processing Standards (FIPS) model [220] of Low (1-5), Moderate (6-10) or High (11-15). The calculation of the risk of an application based on a single security objective is represented by Rs, which is the average over the cumulative weighted sum of n threats which map to a particular SO category.

$$R_s = \frac{1}{n} \sum_{i=1}^{n} P_e I_e \tag{6.5}$$

So for example, in assessing the risk of a cloud service, let us assume that three threat events were identified and they all related to the confidentiality SO, i.e. cross-site scripting (XSS) attack, malicious access to API keys and man-in-the-middle attack. These threats were estimated to have impact (I) values of 3, 7, 10, and the probability (P) of their occurrence are 0.08, 0.1, 0.24. Therefore, the risk value for the cloud system under the confidentiality SO would be [0.08(3) + 0.1(7) + 0.24(10)]/3 or **1.11**. Due to the combined

value of risk under the same SO, the confidentiality risk of the cloud service will be classed as a low risk, seeing that it is far below the maximum potential risk value of [1.00(10) + 1.00(10) + 1.00(10)]/3 or **10**.

Furthermore, the net security risk (R) for the cloud application will be represented below as the weighted average of the risk calculated for the CIAMAU objectives.

$$R = \sum_{s=1}^{6} w_s R_s \tag{6.6}$$

where the ws for the CIAMAU SOs could have values similar to [0.3, 0.1, 0.1, 0.2, 0.1, 0.2].

In summary, the RA steps identified in the QUIRC model promote communication on risk factors between external experts and internal stakeholders. The model also enables CSPs to consider how identified threats, impact business objectives. The QUIRC is adaptable, and its use can be extended beyond cloud computing to other IT and technology industries, where there is access to subject matter experts (SMEs) and industry-specific knowledge-base. However, its use of a Delphi method for impact estimation is bound to slow down the risk assessment process, and the ability of the CSP to adapt to risks in the cloud. It is easy to see RA exercises taking over a month to complete since issues relating to expert consensus, and expert/ stakeholder availability need to be considered. Also, the QUIRC model fails to consider the direct and indirect consequences of an impact from their suppliers.

6.8.2 CSPRAM

In [19], Albakri et al. proposed a security risk assessment method for cloud computing environments. This framework contains several components, including a cloud service provider risk assessment manager (CSPRAM). It is designed to be used by CSPs in assessing the security risks in their cloud computing environment and is complemented by the inclusion of customers' evaluation of security risk factors [19]. This study addresses the challenge of defining the risk criteria according to the organisation's security objectives and considering these criteria when evaluating the value of a risk event. The model also includes cloud customers (CC) in the risk assessment process. The inclusion of customers is limited to processes that define the security risk factors, such as asset value, the likelihood of a threat, vulnerability, and impact of the incident, as well as determining the legal and regulatory framework. However, the authors maintain that including all CCs can quickly become unmanageable if all their objectives are included in the risk evaluation.

The CSPRAM model follows the ISO/IEC 27005 standard in defining its main risk assessment steps. The authors defined risk as a combination of the likelihood of a threat and the impact of the incident. The framework is made up of two main parts: The CSP and

CC assessments. It attempts to achieve a balance between the *realistic result* obtained from the contribution of the customer, and the complexity of the risk assessment process due to the inclusion of the CC. The risk analysis phase takes into consideration the information provided by the CC and CSP's knowledge of their threats, vulnerabilities and controls. Subsequently, the CSP determines the risk level based on the likelihood of the incident scenario and its consequences and compares the risk levels with the risk evaluation and risk acceptance criteria set at the beginning of the process, producing a prioritised list of risks.

CSPRAM is designed to assess the risk of a cloud service (particularly SaaS), and it uses a risk analysis matrix for rating risk factors. The range of both likelihood and business impact are: very low, low, medium, high and very high. The combination of likelihood and impact values is represented on a risk scale that ranges from 0 to 8. The risk scale is mapped to a simple overall risk rating of LOW (0-2), MEDIUM (3-5) and HIGH (6-8). For example, using table 6.7 to assess the risk of a Distributed Denial of Service (DDoS) attack disrupting the availability of a cloud service requires the assessor to estimate the business impact of the threat and the likelihood of the attack. Estimating the *business impact* as a medium and the *likelihood* of the incident as low, will give us a *risk value of 3*, same as an event with an impact of very low, and a likelihood of high.

Table 6.7: CSPRAM Risk Analysis Matrix

	Likelihood of incident scenario				
Business Impact	Very low	Low	Medium	High (likely)	Very high
Very low	0	1	2	3	4
Low	1	2	3	4	5
Medium	2	3	4	5	6
High	3	4	5	6	7
Very high	4	5	6	7	8

Overall, the CSPRAM model promotes trust between the CSP and customer based on customer involvement in the RA process. Although, determining which customer to pick for the exercise, and deciding on how to manage different customer preferences and risks, could lead to the increased complexity of the cloud hosting infrastructure. The process is also reliant on customers providing accurate feedback, and could also be slow in adapting to the dynamic changes in the cloud ecosystem. The compliance of the model with the ISO27005 standard helps with the scope and boundary definition, but its use of a risk matrix in evaluating different risk scenarios could lead to unprioritised high impact risk events.

6.8.3 OPTIMIS

Djemame et al. [89] proposed the Service Provider Risk Assessment Tool (SPRAT) and Infrastructure Provider Risk Assessment Tools (IPRAT) for cloud service provisioning, and

as part of the EU-funded project, OPTIMIS (Optimized Infrastructure Services). The SPRAT and IPRAT are independent parts of the risk assessment framework. The objective of the OPTIMIS project is to enable an open and dependable cloud service ecosystem, which provides technological assurances. This should consequently lead to higher confidence of cloud consumers and promote the cost-effective and reliable productivity of CSPs and resourcefulness of Infrastructure Providers (IP). The framework aims to deliver flexible, auditable, reliable, sustainable, secure and economical cloud services.

The risk assessment process follows a use case scenario to determine which assets will be involved in the assessment and their interactions. Risks are also assessed by categories (e.g., technical, legal, policy and general) to streamline the mitigation strategies. Using this framework, the different business level objectives of the SP and IP actors, play a part in deciding the importance of cloud risk. The model supports the assessment of cloud risks involved in the outsourcing of a service to an external provider, e.g. infrastructure hosting. Another decision supported by the model is the evaluations of the reliability of IP offerings and their ability to meet stipulated SLA. The suggested use cases supported by the risk assessment framework include: i) private cloud, ii) bursting, iii) multi-cloud, iv) federated cloud, and v) brokerage. Each risk assessment exercise conducted by the SP will incorporate provider reliability into the risk model, to verify the expected integrity of the provider's guarantee when making SLA offer.

The OPTIMIS model defines risk as the combination of the likelihood of an event occurring, and the negative consequence/impact of the undesirable event. For each risk event, the assessors estimate the risk level based on the impact and likelihood of that risk. The likelihood and impact values are labelled from 1 to 5 according to their intensity (1-very low, 2- low, 3- medium, 4- high, 5-very high), and the resulting risk level ranged from 1-25. In Table 6.8, we present an example of a cloud risk event involving the unauthorised access to data due to access to unprotected passwords. Here, the risk assessors estimate the likelihood of the risk as High, which is equivalent to a value of 4, and the impact also estimated as High (4). The resulting risk is a product of the impact and likelihood, which yields a risk level of **16**, with the maximum being **25**.

In summary, the OPTIMIS model provides a good foundation for a reliable and trustworthy cloud environment, seeing that it involves the infrastructure and service provider in the RA process. Using the toolkit, the model can support the frequent assessment of cloud provisioning risk. However, its assessment of cloud risks using predefined use-case scenarios means that any scenario not included in the framework, will not be considered. This model requires a significant level of transparency between the IP and SP, as part of determining the reliability of providers and their ability to meet SLA.

Table 6.8: Presenting a risk event with SPRAT

Risk Category:	**General**
Asset identified	Security
Vulnerability of Asset	Unprotected password
Threat to the Asset	Unrestricted access to data
Resulting risk item	Data leaks
Risk Likelihood	High (4) [Range 1-5]
Risk Impact	High (4) [Range 1-5]
Resulting Risk level	Risk Likelihood * Risk Impact = 4*4 = 16 [Range 1-25]
Risk Event	System hacks
Resulting Risk Mitigation	Encrypting data

Table 6.9: Systematic evaluation of cloud risk assessment models

Models / **Criterion**	**QUIRC**	**CSPRAM**	**OPTIMIS**	**CSCCRA**
Goal	Assessing cloud risks based on security objectives	Assessing the risk of cloud services, with inputs from cloud consumers (CC)	To enable cloud providers analyse and address risk factors in a cloud ecosystem	To enable CSPs identify, analyse and evaluate cloud risks from a dynamic supply chain perspective.
Risk Assessment steps	The RA process is split into two phases : impact assessment using wide-band Delphi method, & probability assessment based on security reports	The model follows the steps defined in the ISO 27005 standard and is split into two aspects: CSP and CC	The RA process follows a use-case scenario in determining the assets and actors required to conduct the assessment. It addresses two cloud stakeholder risks : SP and IP	The model builds on existing RA standards and involves the mapping of a cloud supply chain, supplier assessment, before the risk analysis phase.
Decisions supported by the model	The model supports business-driven assessment of the security of cloud services	Supports the implem-entation of appropriate security controls based on changing customer requirements	The model supports the assessment of risks involved with the outsourcing of a cloud service to an external provider	The presentation of cloud risks in monetary value promotes cost-effective risk mitigation and optimal risk prioritisation.
The scope of risk assessment	The CSP conducts the assessment with help from experts. The model is applicable to other IT systems beyond the cloud.	The scope is reliant on the CSP and how much they choose to include customers in the assessment. The model also includes elements of risk management processes.	The assessment involves both service provider and infrastructure provider. The model extends beyond RA to include risk mitigation and monitoring steps	The CSP conducts the analysis following the assessment of the security posture of their suppliers. The model is extensible to any composite IT service.
Risk Conceptual-isation	Risk (score) = Impact * Probability	Risk (score) = Impact * Likelihood	Risk (score) = Impact* Likelihood	Risk (cost) = Impact * Probability* Frequency

6.8.4 Discussion and Findings

As one can imagine, the three cloud risk assessment models compared in this study are not the only conceptual models available to CSPs. Nevertheless, they were chosen because they were the only ones that met our criteria, as mentioned previously. The work of Fito et al. [105] stands out as another suitable alternative, except for their concentration on business-level objectives and the lack of emphasis on security risks in the application of the SEmi-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) model in a CSP environment. Some of the excluded papers did not give a practical example of the model's application [190, 334], while others did not explicitly consider the supply chain [278, 289] in their risk assessment process.

While each of the discussed models was developed for assessing cloud service provisioning risks, they differ in their primary goal and the process involved in achieving these goals. We draw particular attention to the CSPRAM model [19], which identified the need for involving cloud customers in the risk assessment process. This was based on the understanding that although the CSP owns the cloud infrastructure and software used to process data, the data is owned by the CC, and only them can provide a realistic estimate of the impact cost. CSPRAM authors, however, were cautious not to involve users in all stages of the assessment to avoid process becoming unmanageable.

Furthermore, the comparison of the models strengthened the notion of a predominance of qualitative risk matrix and semi-quantitative risk scoring in cloud risk assessments [14, 167]. A possible explanation for this approach is that their proponents are interested in simplifying the model. However as noted in [258], qualitative approaches can be subjective, and assessments conducted with such methods may often fail to maintain internal and external consistency with the meanings and proportionality of the values used for risk estimation. Such assessments will need to include organisationally-meaningful annotations since their values and meanings are not maintained across other contexts.

A significant aspect of the models discussed is their use of experts. Of the four models discussed in this study, only QUIRC actively makes use of external experts during the impact assessment of cloud risks. Although the deductive risk modelling approach is valuable to the risk analysis process, since it relies on experts' experience, logic, and critical thinking, the QUIRC's wide-band Delphi format makes this model inflexible to address the dynamic cloud risks. Likewise, on the subject of involving members of the supply chain in the assessment of risks, both OPTIMIS and CSCCRA involved suppliers of the cloud service, while CSPRAM involved the customers. Arguments for both approaches can be made. However, a more significant concern will be for CSPs to consider data processing and treatment, particularly when in possession of third-party vendors, given the limited insights CSP's have about

vendor security controls. We, therefore, conclude that the CSPRAM model would have been more convincing if the authors had also considered the "upstream" supply chain.

Similarly, considering the flexibility and adaptability of the models to different cloud scenarios, it would appear that QUIRC is the least flexible. The main reason for this conclusion is because of its need for Delphi participants, which is less adaptable for the cloud. However, the RA approach described in CSPRAM, which the authors claim will be tested in a public cloud SaaS application, does not seem to fit that environment. We maintain that the approach will be more suited to a private cloud setting, where the CSP has a working relationship with cloud customers and can rely on them to be involved in such a rigorous cloud assessment. Lastly, proposing a risk assessment model without a measure of its capability does not assure its effectiveness. As such, we commend the implementation of the OPTIMIS model as a tool and the illustration of its use in assessing cloud service provision risks.

Given that one of the primary purposes of risk assessment is to prioritise cloud risks, that is, decide before a security event which systems are critical to cloud operation, and present this information to the business owners, it is only appropriate for the value of risk to be presented in a format that decision-makers can understand. The CSCCRA model presents decision-makers with a pictorial representation of their risk landscape and helps them to identify weak suppliers within the chain. In their review of a dynamic model, Ghadge et al. [116], maintain that the process of identifying the potential weak spots through the implementation of models capable of capturing the vulnerability in the supply chain is beneficial to practitioners in proactively mitigating the risks. Additionally, while other risk assessment models ignored uncertainty and its associated challenges to simplify their decision-making, the CSCCRA explicitly considered uncertainty in its risk factor estimation, making it an integral part of the model.

Overall, this study has found that conceptual models increase justifiability by making the internal operations of the risk assessment easier to understand for both the assessors and stakeholders. Since cloud risk assessments often involve internal and external stakeholders who have expertise in different domains, the best approach to conducting cloud assessments will be to have all assumptions about the asset and environment documented. This is an area where the CSCCRA model outshines the other reviewed model. Its quantitative and supply chain-inclusive approach enhances the justifiability of risk results and ensures that the risk assessment process is transparent, repeatable and understandable.

Chapter 7

Model Validation using Case Study

In the previous chapter, we described our proposed conceptual model for cloud risk assessment, expanding on its components, assessing its completeness, comparing it to other conceptual models, and reviewing the expert validation process. In this chapter, we discuss the application of our model to assessing the risk of SaaS providers, which also provides answers to research questions RQ3 & RQ4.

As previously discussed, our choice of a multiple-case design is because it lends itself to theory testing [40], which through a cross-case analysis could result in more general research results. We scope the context within which we will rigorously validate and investigate the usefulness and applicability of the designed risk assessment model to three small or medium-sized cloud providers that deliver SaaS cloud applications. The decision to apply the model in assessing provider risks in a real-world context, not only gives us insight into the capabilities of the model, but it also allows for a more thorough and detailed evaluation of the model's proposals within organisations where it matters most. We chose three cases to achieve a deliberate and contrasting comparison among cloud providers who operate in different settings.

Before each case study and in preparation for our data collection, the researcher contacts a technical stakeholder within the CSP organisation, to discuss the details of the study and gather initial data on the SaaS application. Collecting known data about the SaaS's supply chain, documentation of supplier information, vulnerability scan report, a data flow diagram and any other information available to the researcher through open-source intelligence enable us to carry a preliminary analysis of the SaaS application. Following that, a meeting is held with the CSP in their office, where we introduce the model to the key stakeholders who will be participating in the study. This pre-work gives us a good head start and assurance of a reliable result at the end of the exercise. The estimated duration of each case study, where the participants go through all the phases of using the CSCCRA model to assess their cloud risk is one day.

In Figure 7.1, we show the different phases of stakeholder participation based on the CSCCRA risk assessment method.

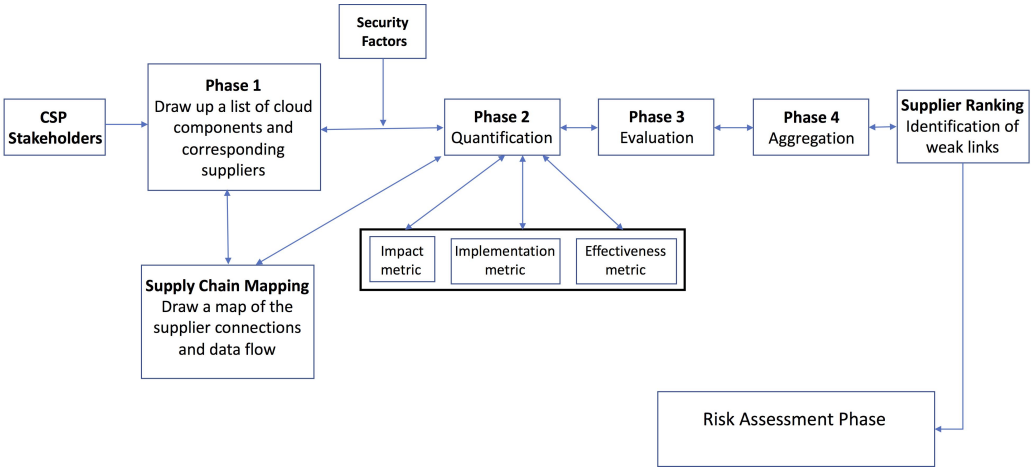


Figure 7.1: Steps taken by case study participants using the CSCCRA model

In the following sections, we describe each case organisation and present and analyse the empirical data collected from them. As part of our analysis, we assess the usefulness and practicality of the model from the following perspectives:

- The ability of the quantitative model to help the CSP think differently about their cloud risks, particularly concerning their supply chain.
- The ability of the model to provide reasonable estimates of risk values, which helps CSP decide on their approach to risk treatment.
- The ability of the supplier security assessment tool to identify weak suppliers and suggest ways of improving the supply chain security posture.
- The potential for the risk assessment tool to be used by both technical and non-technical members of an organisation.

7.1 Case Organisation One - CSP-A

7.1.1 Background of CSP-A

Due to confidentiality reasons, the first case organisation is referred to as CSP-A. CSP-A is an innovative and rapidly growing software company in the south-east region of England. The company was established in the early years of the Internet revolution, and it boasts of staff strength of between 51-250 employees. They are involved in the development of software products used in the health, engineering and science industries. They also work with local government authorities to deliver the services required for social care. In 2016,

they developed a not-for-profit SaaS application aimed at curbing social isolation across different age groups, which is the focus of this case study.

We completed this case study on the 21st of September 2018. We approached CSP-A to take part in the study because a principal member of their team had participated in our previous study. However, it seems they obliged because, at the time of our asking, they were also preparing to conduct a risk assessment of the application in compliance with a European Union (EU) grant. In our invitation to them, we gave CSP-A a background on cloud risk assessment and the gaps in literature and practice, which we have identified as part of our research. Following that, we introduced our proposed model to them, highlighting its benefits.

After CSP-A agreed to participate and before arranging a date for risk assessment exercise, we met with three key stakeholders (two technical & one business) of the SaaS application to brief them about the model and confirm it was a good fit for their application. We identified what we required of each stakeholder as part of the assessment and provided them with a projected plan and the expected duration of the exercise (i.e. one day). In the following section, we describe the activities of the risk assessment exercise and the result of the assessment.

7.1.2 Application of CSCCRA to CSP-A-SaaS

Conducting a case study can be an intensive process, one that requires a detailed collection of data before the exercise [294]. Our initial data collection saw us gather data on the SaaS applications' components including services such as DNS, Web Hosting, E-mail, Database, Payment and Identity and Access Management, and identify their suppliers. We collected this information from external information sources such as the technology lookup website, builtwith.com [52] and Google. Using the information gathered, we created a draft of CSP-A's SaaS supply chain map identifying some of their suppliers. This unique effort fascinated the stakeholders and gained us their support for the duration of the exercise. A total of six participants took part in the risk assessment exercise; three participated in all the exercises, while the other three were called upon during the risk estimation stages since they were more aware of the business impacts of risks (see Table 7.1). In the following sections, we apply the CSCCRA model to assess the risk of the CSP-A-SaaS application.

7.1.2.1 Supply Chain Mapping

The process of assessing cloud risks with the CSCCRA model follows the steps identified in Figure 7.1. Presenting the stakeholders with the initial information collected, we got them to provide the other components, which were not externally visible. Throughout the exercise, we made references to build guides, supplier web portals and made use of search

Table 7.1: List of Participants for Case Study One

No.	Stakeholder	Role	Extent of Participation
1.	Participant-A1	Infrastructure & Security Director	Supply chain mapping & Risk estimation phase
2.	Participant-A2	Systems & Security Administrator	Participated in all phases of the study
3.	Participant-A3	Product Manager	Participated in all phases of the study
4.	Participant-A4	Managing Director	Risk estimation phase
5.	Participant-A5	Project Manager	Risk estimation phase
6.	Participant-A6	Systems Administrator	Participated in all phases of the study

engines to ensure the information used for the assessment were current and accurate. Figure 7.2 presents the anonymised supply chain map of CSP-A-SaaS (i.e. the SaaS application). Likewise, in Table 7.2, we identify the cloud components, suppliers and service category, their criticality, and the data storage or processing responsibilities of the supplier.

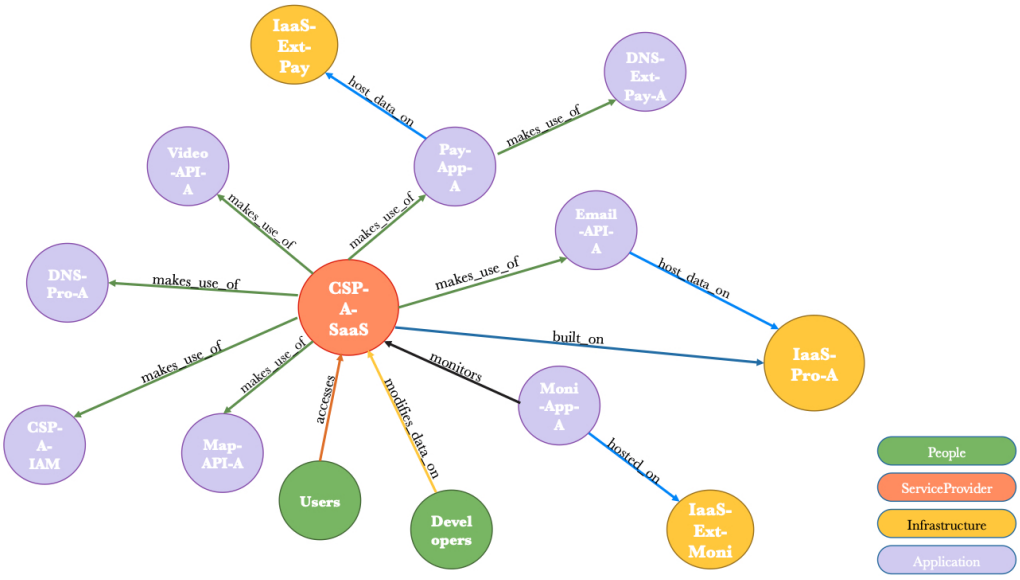


Figure 7.2: Supply Chain mapping of CSP-A-SaaS using the CSCM tool

Visualising a supply chain helps to detect convergence risks, where a critical supplier in the second, third or fourth tier could represent a single point of failure for multiple components of the cloud service. We did not go into greater detail on the lower tier suppliers, due to the unavailability of information on some, and because, most of the component providers, where themselves IaaS providers, who are assumed to host the applications internally. Nevertheless, as shown in Figure 7.2, the use of a visual structural model helps to illustrate the interdependencies between the components and accurately visualise the cloud information flow. Here we see that CSP-A-SaaS relies on IaaS-Pro-A not just for its hosting function,

Table 7.2: CSP-A First-tier Supplier list

Anonymised Supplier	Component	Service Category	System Criticality	Data Proce-using (Y/N)	Data Stora-ge (Y/N)
IaaS-Pro-A	Hosting (Web, Code), Database & Backups	Application/ Infrastructure	Very Critical	Y	Y
CSP-A	*IAM & Software code*	*IAM, Software development*	*Critical*	*Y*	*Y*
Email-API-A	E-mail	Application	Critical	Y	Y
Video-API-A	Video	Application	Not Critical	N	N
Map-API-A	Maps	Application	Critical	N	N
DNS-Pro-A	DNS	Infrastructure	Very Critical	Y	Y
Moni-App-A	Monitoring	Application	Not Critical	N	N
Pay-App-A	Sales and Billing	Application	Not Critical	Y	Y

but there is also an indirect dependency on the provider for email services.

7.1.2.2 Supplier Security Assessment

Using the information identified in Table 7.2 and aided with a visual structure of the SaaS's supply chain (Figure 7.2), we proceeded to the next phase of the assessment, i.e. supplier assessment. As previously described, the CSSA tool empowers CSPs to assess the cybersecurity posture of cloud suppliers. It assists CSPs to evaluate each supplier's security posture by presenting them with a consistent approach to assessing and comparing suppliers based on our nine (9) security target dimensions.

The supplier assessment phase took about 2.5hours, longer than the time initially allotted (1.5hrs), because the participants did not have enough information on their suppliers, and had to rely on observation and publicly available information. While this experience supports the lack of visibility of provider controls, which we have argued has contributed to the lack of comprehensive cloud risk assessments [11], it also confirms an element of blind trust with cloud customers. According to Chan et al. [59], the challenge organisations face in obtaining the desired information for a thorough risk assessment has led many cloud customers to blindly trusting the provider, and passively accepting providers' report on the security of their service. This suggests that, while the information suppliers provide on their security controls do not necessarily translate to what they do in reality, we are forced to accept it. Werff et al. [327] highlight the advantage of cloud trust built on the knowledge of CSPs processes, architectures, and visible controls over the trust based on the calculation of potential costs and benefits. For this reason, it is appropriate to continue to encourage CSPs to find out more on their suppliers before engaging with them.

The result of the supplier security assessment using the CSSA tool is presented in Table 7.3.

Table 7.3: Assessing CSP-A Suppliers using CSSA

Anonymised Supplier	**AoS (1 -10)**	**DSH (1 -10)**	**DSC (1 -10)**	**MSA (1 -10)**	**MOS (1 -10)**	**SGC (1 -10)**	**IAM (1 -10)**	**EKM (1 -10)**	**AS (1 -10)**	**Combined Z-Score Value**
IaaS-Pro-A	8	10	10	10	10	10	10	9	9	-0.20
CSP-A	*7*	*9*	*9*	*8*	8	*8*	*9*	*9*	*9*	*1.28*
Email-API-A	10	9	10	10	9	9	10	10	9	-0.17
Video-API-A	9	10	10	9	7	7	9	9	9	0.65
Map-API-A	9	10	9	10	8	10	10	10	9	-0.07
DNS-Pro-A	10	10	10	10	10	10	9	10	10	-0.71
Moni-App-A	10	10	10	9	10	10	10	10	9	-0.46
Pay-App-A	8	10	10	10	9	10	10	10	9	-0.31

As shown in Table 7.3, the participants' scoring rated CSP-A as the weakest link of the supply chain, one with a high susceptibility to a cyber attack. While this supports the objectivity of the participants, it also shows that in circumstances where limited information is available to customers, they lean towards "blind trust" [11, 57]. As part of this study, the researcher observed situations where participants did not have details of a supplier's security control or operational process, and they coerced themselves to score the suppliers high, stating that they had no choice. However, according to Raj Samani [248], in cases where an organisation is not transparent about the maturity of their risk management, our level of assurance of such organisation should decrease.

CSP-A scored themselves low in areas where they lacked adequate controls around the components they managed. Some specific areas where gaps were noticed included DR, backup and storage, authentication (No MFA), encryption and continuous security assessment. While CSP-A was honest in their assessment of their abilities as the focal SaaS and sometimes hard on themselves because they believed they could improve, the same cannot be said for all cloud suppliers. However, seeing that we were unable to bridge the information asymmetry gap, the scoring was made to best-effort. Other factors considered during the assessment of suppliers includes their history with CSP-A and their reputation. One of the suppliers that CSP-A had contracted based on its reputation was the next weak supplier - Video-API-A. For this supplier, we found little information about their processes, outside the general security controls, but since they stored no critical data, they were judged as minimal risk. The supplier (Pay-App-A), who despite being part of the payment industry, provided valuable information on their processes. In the course of this assessment, we found out some of their worthy endeavours to promote secure service delivery, one of which was their bounty scheme for detecting security vulnerability in their application. Although the participants were not aware of these findings before they signed up with the provider, they were encouraged by the news.

Overall, the participants found this supplier assessment enlightening, considering its rigorous approach which required them to look through their documentation (of which there was little) and search online for details about their suppliers. From our observation, it seems

the details most providers have about their vendor are restricted to compliance, availability and other SLA-related information. Information on technical or operational security is often limited. However, we believe that the exercise made CSP-A aware of their lack of information on suppliers that were critical to their application. One of the participants even suggested that they *would look into including all their suppliers in their upcoming ISO/IEC 27001 assessment*. This recognition is a positive outcome of this study and one that meets our goal of causing CSPs to step back cognitively from their usual approach to risk assessment and fundamentally question and rethink their established interpretations of situation and strategies.

7.1.2.3 Quantitative Risk Analysis

Following the structured approach of the CSCCRA model and having completed the rating of the cybersecurity posture of each supplier, comparing them to one another, we progressed to the quantitative risk assessment stage. This phase began with a powerpoint presentation on quantitative risk analysis and risk estimations. At the end of the presentation, the participants were given a short calibration exercise, to prepare them for making reasoned estimates about the risk factors identified in the course of the assessment. To avoid subjective confidence (over or under), synonymous with estimation, we provided the participants with information on how to estimate values to a 90% CI. 90% CI means that for each estimate provided, there is a 5% chance of the answer being less than the lower bound, and a 5% chance of the answer being higher than the upper bound. Hubbard [142] and Freund & Jones [112] gave insights into conducting proper risk estimations by calibrating the expert team. So in this exercise, we presented the stakeholders with six general knowledge questions and got them to estimate the answers to a 90% CI. The responses of the participants were not overly subjective, and so we proceeded with identifying the risk of the application.

Considering that this application is for a non-profit purpose, CSP-A prioritised confidentiality risks over availability and integrity ones. CSP-A acknowledged the impact attacks such as customer data breach could have on their brand name, reputation and continuous patronage from their other paying customers. As such, CSP-A set a goal for us to assess the security risks of this web application and provide steps that could be taken to mitigate the risks. The risk identification step of the process looked to identify and prioritise the risks of CSP-A-SaaS, such that, at any given moment, ten or less high priority risks are being tracked on the risk register. So, from the vantage point of the just concluded supplier security assessment and the supply chain mapping, the participants were able to visualise their areas of weakness and begin to identify vulnerabilities, threats and probable risk events.

Table 7.4 shows the top ten risks identified in the course of the exercise. The risk registry is a table that lays out: a description of each risk, the asset at risk, suppliers involved,

vulnerability, threat agent, threat type, security effect and available control. The threat, vulnerability, asset taxonomy complies with ENISA's method of structuring risk information [58, 196]. With each identified risk likely to have more than one threat agent, security effect or vulnerability, our risk analysis approach chose the scenario we believe represented the most likely and costly to the business and analysed it. We realise our inability to conduct a 100% comprehensive measurement of risk, hence we settled for pragmatically reducing uncertainty around risk events and having enough information to mitigate the top risks. We focused on the asset-level controls put in place to prevent risk or reduce the effect of its occurrence and discussed ways of improving the controls.

As mentioned in the methodology, we adopted a participatory research method. So, in preparation for the risk factor estimation and quantitative analysis of CSP-A-SaaS, we proposed three ideas to the participants: i) assume this has been measured before; ii) by being resourceful, you can find more data; iii) you need less data than you intuitively think you need [142]. We informed them of the need to make all estimates to a 90% CI, similar to the calibration exercise. They were to consider the results of the initial stages of the assessment in their estimations to improve their objectivity. Each participant was to provide an independent estimation of the probability, frequency, impact cost and evaluation of countermeasures for each risk item. The estimates for the probability (with or without control) and impact cost were to be presented in a probability distribution, including the LB, ML and UB estimates, while the frequency factor was based on the average rate of occurrence. Similar to the FAIR method, some of the factors accounted for in the estimation of impact cost includes: operational disruption in revenue generation (productivity cost), response costs (notification of customers, customer support), replacement costs (root cause analysis, dealing with law enforcement), and other legal and public relations (PR) costs [112]. Likewise, the probability of occurrence estimates the success of a threat agent exploiting a vulnerability, considering the controls.

Considering that some of the risks were related to fines, response and reputation losses, our full-time participants (A2, A3 & A6), had to consult with their colleagues (A1, A4 & A5) who work more on the business side to quantify the impact cost. We gathered from this singular act that, stakeholders find it difficult to assess the impact of a risk on an organisation, particularly when it relates to loss of customers and reputation. On completing the estimations, the researcher gathered the data and analysed each risk item using our Monte Carlo simulation tool. We follow the example of the risk calculation carried out in Section 6.3 to build models of possible risk results based on the estimations of the risk factors. Each risk result was calculated over five (5) simulations of a hundred thousand (100,000) iterations each, producing a distribution of possible risk values for a particular risk item. Additionally, and as a rule of thumb during our analysis, we applied a mental

Table 7.4: List of Security Risks identified by the CSP-A Stakeholders

Risk No	Risk Description	Asset at Risk	Supplier	Vulnerability Name	Threat Agent	Threat Type	Security Effect	Existing Controls
R1.	Loss of CSP-A-SaaS assets due to an unauthorised access to the hosting platform	Personal data, Intellectual Property, source code, backups	IaaS-Pro-A, CSP-A	Insufficient Identity and Access Management (No Two factor (2FA), misconfigured access control), No encryption at rest	Malicious Outsiders, Privileged Insiders, CyberCriminals	Sabotage, Social Engineering, Unauthorised Activity, Abuse of Authorisation	Confidentiality, Integrity, Availability, Reputation	Role-Based Access Control (RBAC), Good password Policy
R2.	Unavailability of service due to DDoS	Service Delivery, SaaS Management Interface	DNS-Pro-A, IaaS-Pro-A, Pay-App-A	Inadequate resource provisioning, Publicly available service	Malicious Outsider	Denial of Service	Availability	Operational Security measures (e.g. monitoring, logging)
R3.	Data Breach of customer PII data	Personal data, Credentials	IaaS-Pro-A, CSP-A	Unencrypted storage of data, Weak encryption of archives and data in transit, Poor key management procedures,	Malicious Outsiders, Privileged Insiders, Accidental Insider	Information leak/sharing	Confidentiality, Privacy, Reputation	Existing data security policies, encrypted data in transit
R4.	Loss of SaaS application data	Source code, Backups, Personal data	IaaS-Pr	Unencrypted storage of data at rest, Inadequate data archiving procedures (Application and backup storage stored with the same provider)	Provider , Malicious outsider, Privileged insiders, Accidental insider, Environmental, Political,	Loss due to administrative error, Sabotage, Theft, Failure of system	Availability, Reputation	Backup restoration Offsite source code repository
R5.	Data breach of customer sensitive and PII data	Personal sensitive data (E-mail), PII	Email-API-A, Pay-App-A	Insufficient Identity and Access Management (No Two factor (2FA), misconfigured, Access control), Insufficient Log auditing	Malicious Outsider	Information leak/ sharing	Confidentiality, Privacy, Reputation	Security and Operational Logging, RBAC
R6.	Data breach of customer Payment Card Industry (PCI) data	Personal data- critical	Pay-App-A	Application/Platform vulnerability, Misconfiguration,	Malicious Outsider	Information leakage	Confidentiality, Privacy, Reputation	Payment provider controls
R7.	Unavailability of service for 6 hours due to software code bug	Service Delivery, SaaS Management Interface, Source code	CSP-A	Non-optimal change and configuration management procedures, Poor patch management, Limited support staff	Insiders	Service outage,	Availability	Available test site, Code release policies, SDLC
R8.	Malicious actors exploit security flaw in the SaaS website to distribute malware to users	Service Delivery	CSP-A, IaaS-Pro-A	Application vulnerabilities or poor patch management, Limited control for file upload	Malicious outsider, Privileged insiders	Abuse and Nefarious use of cloud service, Malicious code	Reputation, Infrastructure	Penetration testing, Following OWASP best practice
R9.	Replacing SaaS web video with unsuitable content	Service Delivery	CSP-A/ Video-API-A	Insufficient Identity and Access Management (No Two factor (2FA), misconfigured access control), No audit log of video API activity	Malicious (outside, insider)	Abuse and Nefarious use of cloud service, Website defacement	Reputation, Integrity	none
R10	SaaS application users unable to access platform for 6 hours due to a Service outage	Service Delivery	IaaS-Pro-A	Provider misconfiguration, No redundancy, Shared platform vulnerabilities	Insider (privileged, accidental), Malicious outsider	Service outage	Availability, Reputation, Infrastructure	Service uptime and outage monitoring, Provider redundancy controls

litmus test to verify if the result of the CQRA simulation appears to be credible considering the participants' estimations. See Table 7.5 for the estimated risk values.

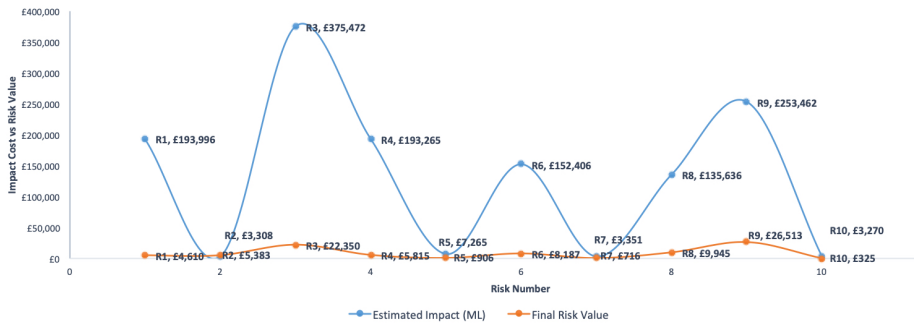


Figure 7.3: CSP-A's Impact Estimate vs. Risk Value Calculation

In Table 7.5, we present the estimated risk value in rounded numbers for easy analysis, which, according to Freund & Jones [112] is also a good way of presenting a risk to decision-makers. Figure 7.3 is a scatter diagram that shows the relationship between the combined stakeholder impact estimates, in this case, the most likely (ML) impact cost and the estimated risk value. What is not shown in the figure is how the other risk factors such as probability and frequency of risk occurrence affect the calculation of the final risk value. For instance, Risk R2, the most likely impact cost (£3,308) is less than the estimated risk value (£5,383) because the average frequency of occurrence for the DDOS risk is estimated to occur twice a year. For more information on the CSCCRA model's sensitivity analysis, see Appendix F.

Our evaluation of the estimated risk value based on existing controls, saw us consider values ranging between the 65% to 90% percentile of the risk value continuum. We did this for a couple of reasons, first was the level of uncertainty around the estimations echoed by a majority of the stakeholders; some of this uncertainty was around the cost of data breach fines (e.g. GDPR) and their limited knowledge of supplier security controls. Secondly, a majority of the risks involved external attackers whose threat capability could be said to be higher than average and an assessment of the existing controls, which in some cases are less optimal. We rated the stakeholders as having moderate confidence in their estimations, and as such, conducted further analysis around CSP-A's existing controls. We also referred back to some of the responses we got from the informal interviews we conducted during the assessment.

For brevity of this report, we have not listed each stakeholder's estimation of the various risk factors, neither have we shown the calculation of each risk value. That is because we believe our earlier example of the step-by-step process used to arrive at a risk value is clear (see Section 6.3 for details). Risk management is a function of an organisation's ability to make well-informed decisions and execute against those decisions over time [112], and we

Table 7.5: CSP-A Risk Analysis result based on CQRA calculation

Risk No	Probability of occurrence (without control)			Probability of occurrence (with control)			Impact Cost Estimate (£)			Frequency (per year)	Risk Value (£) Estimates (without controls)			Risk Value (£) Estimates (with controls)			Estimated Risk Value (£) based on Existing Controls
	LB	ML	UB	LB	ML	UB	LB	ML	UB		LB	ML	UB	LB	ML	UB	
R1.	1.70%	6.70%	16.00%	0.50%	2.20%	4.40%	£91,852	£193,996	£391,144	0.10	£0	£5,722	£31,293	£0	£1,909	£10,144	**£4,610**
R2.	1.40%	14.40%	39.40%	1.00%	4.20%	9.20%	£897.85	£3,308	£6,290	2.00	£0	£9,676	£54,495	£0	£2,833	£12,344	**£5,383**
R3.	1.80%	8.90%	15.50%	1.70%	4.40%	7.50%	£71,472	£375,472	£818,308	0.50	£0	£18,617	£91,942	£0	£9,546	£45,704	**£22,350**
R4.	1.00%	7.50%	14.30%	1.10%	3.90%	7.40%	£97,168	£193,265	£390,186	0.58	£0	£8,241	£40,347	£0	£4,379	£21,103	**£5,815**
R5.	4.08%	9.07%	15.96%	3.09%	5.80%	11.39%	£2,487	£7,265	£14,657	0.50	£0	£335	£1,656	£0	£212	£1,053	**£906**
R6.	1.11%	10.49%	32.43%	1.03%	4.86%	12.40%	£24,703	£152,406	£386,531	0.45	£0	£7,050	£41,834	£0	£3,272	£19,080	**£8,187**
R7.	12.89%	20.81%	28.84%	5.23%	10.08%	16.32%	£919	£3,351	£7,067	1.28	£0	£897	£3,137	£0	£436	£1,522	**£716**
R8.	3.60%	12.53%	24.45%	1.14%	3.25%	7.81%	£24,926	£135,636	£375,442	0.52	£0	£9,004	£48,497	£0	£2,329	£12,054	**£9,945**
R9.	1.52%	4.71%	12.77%	0.51%	3.99%	12.69%	£40,994	£253,462	£790,873	0.45	£0	£5,063	£26,888	£0	£4,502	£22,303	**£26,513**
R10.	5.41%	9.20%	17.88%	1.06%	4.11%	11.39%	£907	£3,270	£6,551	0.80	£0	£245	£971	£0	£109	£516	**£325**

believe our assessment provides decision-makers with quality information, simplifying the process of risk mitigation. Bearing this in mind, we presented CSP-A with a risk assessment report highlighting the assessed risks and their estimated values, as a way of compensating them for the time spent on the case study. The report also contains a risk treatment section, where we identified best practices that can be implemented to mitigate the risk scenarios. In the following section, we discuss elements of the evaluated risks and confirm the risk treatment actions.

7.1.3 Analysis and Discussion of Assessment results

This case study set out to assess the risk of a SaaS application using the CSCCRA model. The evaluation is aimed at demonstrating the applicability and feasibility of the model and validate its use within a real-world context. To recap the case data, assessing cloud risks using the proposed model, consists of three phases. In the first phase, stakeholders identify the components of the cloud service and map out their full supply chain using the CSCM tool. Next, they assess the cybersecurity posture of their suppliers based on nine target security factors, to identify areas of weakness within the chain and how this could directly or indirectly impact them. Finally, stakeholders identify the top ten risks of the SaaS application and use the CQRA tool to assess the risks, presenting the value of the risks in monetary (£) terms. Although these results can be further improved by gathering more data and spending more time with the stakeholders, the ability of the team to complete this assessment within an 8-hour day is quite commendable.

During the assessment, we identified some opportunities for security control improvements, some of which are common across multiple asset types (e.g. Logging and MFA). The information we gathered from interviewing the stakeholders during the exercise showed that the CSP did not conduct a comprehensive evaluation before each of the suppliers identified in Table 7.2, were selected. Some of the factors considered in choosing the suppliers included "availability of free credit", "provider reputation", "past working experience", "recommendation" and "ease of setup". Therefore, the CSP had limited information on their suppliers, which was evident during the supplier criticality and cybersecurity posture assessment. Here, the stakeholders had to think through some of the supplier functions critically, because they were not apparent, and possibly not considered in the overall security plan of the cloud service. As shown in Table 7.4, risk in the context of CSP-A's business can be seen to lie primarily between a few suppliers (IaaS-Pro-A, CSP-A, & Pay-App-A), but this could not be verified, as there was no recent vulnerability assessment (VA) scan report. Ideally, the VA report should have fed into the risk assessment process, helping us to focus on areas of high and critical risks, instead of considering all risks in general. Nevertheless, a reasonable assessment of each of the supplier controls was carried out.

Taking a look at the list of identified risks, we see that a majority of them lie within the confidentiality and availability risks, and had a reputational impact on CSP-A. CSP-A, however, prioritised confidentiality risks over availability and integrity ones, because of its financial impact on their business, either as part of a fine or loss of reputation. This perhaps resulted in the noticeably high impact estimations of specific risk items even though their probability of occurrence were quite low. Risk **R3**, which considered the data breach of customer PII data based on an attack on IaaS-Pro-A and CSP-A, was ranked highest in the impact estimations. Two stakeholders had the upper bound impact cost at £1,200,000 & £1,615,000 respectively. Nevertheless, this risk has a low frequency of occurrence, estimated to occur once in 2 years, bringing its overall rating to a MEDIUM risk. To avoid such significant fines, which are often levied on data processors that fail to demonstrate the processes implemented to guarantee data protection and compliance, CSP-A is advised to put in place preventive and responsive controls that ensure irregular activity is detected within their infrastructure and the correct team notified. Also, risk **R1**, which is categorised as a LOW risk, based on the difficulty for an attacker to pull off, is one risk that could disrupt the entire cloud service. Seeing that CSP-A lacks some best practice controls around authentication, logging and encryption, which exposes them to some of the 2018 OWASP top 10 web application vulnerabilities [233], this assessment of the risk, justifies the need for the improvement of the existing controls.

The risk value estimations of risks **R5** & **R6**, which are data breach attacks on the payment provider (Pay-App-A), is worth discussing. While one will think these two risks should ideally command a high impact cost estimation, they have been rated relatively low, due to the arrangement in place for the delivery of the service. For risk **R6**, CSP-A relies solely on the controls in place at Pay-App-A, which in some cases might not be sufficient. Furthermore, when asked about the low impact cost estimations, one of the stakeholders confirmed that they were not going to be liable for the fines against the payment provider, and they will most likely be hit by reputational loss and other public relations (PR) cost. This is because, post-GDPR, data processors (e.g. payment provider) can now be held accountable by the Information Commissioners Office (ICO) and the data subject, for certain aspects of personal data processing [198].

Other risks such as the defacement of the SaaS website (**R9**), unavailability of the service (**R7** & **R10**) and **R8** - a risk scenario where malicious actors using CSP-A-SaaS as an attack vector, were considered. Risk **R8** was a surprising addition to the risk register, seeing that it is an often-overlooked phenomenon in IT risk assessment, i.e. a risk event where the focal asset (an item of value) is a threat agent [258]. In this case, CSP-A-SaaS spreading malicious content could easily hurt other members of the supply chain and CSP-A's business. However, as we see from Table 7.6, CSP-A had no asset-based security control

addressing such risk.

7.1.3.1 Risk Mitigation and Treatment Recommendation

Here, we present controls that could mitigate or eliminate the identified risks and improve CSP-A's operations in the cloud. We consulted cloud security best practice documents [98, 267], identifying security controls that addressed each risk item and presented them to CSP-A to determine their risk treatment plan and nominate a risk owner (see Table 7.6). Based on CSP-A's existing controls, some of our suggested improvements included: (i) improving on the privileged access management; (ii) improving operational security (redundancy, event notification); (iii) improve data classification, protection and encryption processes; (iv) deploy web application firewalls (WAF); and (v) conduct privacy impact assessment.

For each of the identified risks, there are four standard risk treatment options (avoid, accept, transfer, mitigate). The two ideal options for the CSP-A-SaaS platform are the mitigation of the risks within CSP-A's remit and the acceptance of other risks relying solely on supplier controls. While risk transfer is an option, it will not be recommended in this case, neither is risk avoidance, except in a case where a supplier is changed for a more secure one. We believe that presenting the CSP with a supply chain map of the SaaS application, the supplier assessment results, the estimated risk values and a proposal for improving their security controls, would provide them with a comprehensive view of their risks and help them decide on their approach to risk treatment.

7.1.4 CSP-A Evaluation of Model and Case Study Exercise

As a concluding part of this exercise, we got the stakeholders who participated fully (3) in the exercise to evaluate our model. Using a set of questions on a five-point Likert scale, we requested that participants rate the model on criteria such as its understandability, usefulness, ease-of-use, decision-making ability, transparency and practicality. We also presented the participants with nine (9) free-text questions requesting them to assess the strengths, weaknesses, shortcomings, practicality of the model, while also suggesting areas where our model can be improved.

Based on the above criteria, the feedback received from the stakeholders was positive (see Figure 7.4). The participants strongly agreed/agreed with the majority of our statements regarding the advantages of the overall model and its components. When asked about the reproducibility of the assessment results, one of the participants was undecided. This response did not come as a surprise, seeing what each participant went through to gather data on their provider, confirm their security controls and estimate the impact of specific risks. That said, we believe that if a different set of experts, who are knowledgeable about

Table 7.6: Treating CSP-A's identified risks based on Best Practice and assigning Risk Owners

Risk No	Risk Description	Existing Controls	Security Best Practice	Estimated Risk Cost	Risk Treatment?	Risk Owner?
R1.	Loss of CSP-A-SaaS assets due to an unauthorised access to the hosting platform	Role-Based Access Control (RBAC), Good password Policy	Improve Privileged Access Management (PAM); Multi-Factor Authentication (MFA) Implement Data Encryption at Rest; Logging and Event Notification; Data Classification and Protection.	**£4,610**	Avoid or Accept or Transfer or Mitigate Policy	e.g. BU01
R2.	Unavailability of service due to DDoS	Operational Security measures (e.g. monitoring, logging)	Deploy Web Application Firewalls (WAF) and other security measures to protect SaaS; Correctly size the web servers hosting application; Improve operational security process by including redundancy options.	**£5,383**		
R3.	Data Breach of Customer PII data	Existing data security policies, encrypted data in transit	Have an Incident response plan and implement an incident handling process; Database Encryption for data at rest; Data breach detection and notification; File and content security.	**£22,350**		
R4.	Loss of SaaS application data	Backup restoration Offsite source code repository	Implement Disaster Recovery (DR) with an alternate provider for the SaaS application to function as a configuration backup or limited functionality environment; Configuration Management.	**£5,815**		
R5.	Data breach of customer sensitive and PII data	Security and Operational Logging, RBAC	Incident response plan; Database Encryption; Cyber Security Awareness Improve Privileged Access Management; Data breach detection and notification; File and content security.	**£906**		
R6.	Data breach of customer Payment Card Industry (PCI) data	Payment provider controls	Independent review of supplier security controls; Request transparency of security controls; Enforce a supplier selection and management process.	**£8,187**		
R7.	Unavailability of service for 6 hours due to software code bug	Available test site, Code release policies, SDLC	Configuration Management; Secure coding best practice; Improved code backup and restore procedure; Regular static and dynamic source code scan.	**£716**		
R8.	Malicious actors exploit security flaw in the SaaS website to distribute malware	Penetration testing, Following OWASP best practice	Regular static and dynamic source code scan; Proactive software patches; Secure code execution environment.	**£9,945**		
R9.	Replacing SaaS web video with unsuitable content	none	Web activity monitoring; File and content security; Incident handling and notification.	**£26,513**		
R10	SaaS application users unable to access platform for 6 hours due to a Service outage	Service uptime and outage monitoking, Provider redundancy controls	Implement Disaster Recovery (DR) with an alternate provider; Proactive assessment of supplier security controls.	**£325**		

the application, follow the structured approach of this model and use the same supplier documentation, they will generate reasonably close risk results.

Some of the areas where the participants suggested improvement in the model include the incorporating uncertainty in the supplier assessment scoring. As one of the stakeholders put it '*consider scoping the definition of the scoring, distinguishing between 'perceived' vs 'known' scores*'. Another participant also suggested that we formally define supplier assessment scores, since experts could quickly resolve to be subjective, if not rightly guided. To these suggestions, we are currently considering solutions to making the scoring more objective, one of which will involve informing participants to apply a consistent approach to their scoring. For example, in situations where there is a lack of information on supplier controls, and stakeholders are forced to make assumptions, they could follow the advice of cloud risk expert, Raj Samani [248], and the cloud security alliance (CSA) [76], to consistently score the supplier low. While other mathematical approaches will be more appropriate, incorporating them into a Z-score model might introduce a new challenge for the participants.

Furthermore, another area where participants required to see an improvement over time is the risk identification phase. One participant suggested having a predefined cloud risk taxonomy to facilitate the systematic and repeatable identification of risks. He suggested this would speed up the risk identification process. However, while this is a welcome suggestion, one which we hope to test in future exercises, we acknowledge that each CSP will have different risks and presenting example risks to stakeholders could prevent them from thinking in-depth about the peculiarities of their supply chain. Nevertheless, we can see the long-term goal of this task, envisioning that it might enable us to build a new cloud risk taxonomy to replace the existing ones, e.g. ENISA [58].

In conclusion, the case study participants' feedback confirmed the applicability of the model to a SaaS CSP and the effectiveness of its decision-making framework. The stakeholders highlighted the usefulness of the model for comparing risks before and after control implementation, its ability to show the 'big picture' and identify areas of weakness in the supply chain or within processes, and how its comprehensive approach improves cloud risk value estimations. Overall, the CSP's willingness to continue using aspects of the model for future risk assessments, confirms the ability of the model to bridge some of the existing cloud risk assessment gaps.

7.1.5 Summary

In summary, this study showed how the CSCCRA model enables CSPs to understand, manage and make well-informed decisions about their cloud risks. It bridges the supply chain and uncertainty quantification gaps of both the generic and domain-specific risk assessment frameworks. A significant take away from this study is the effect of supply chain

Criteria	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Supply Chain Mapping (CSCM)					
The CSCM tool is a good first step in the risk assessment process	♦ ♦ ♦				
Identifying and mapping your cloud supply chain enables you to visualise data flow, and assists in thinking about security (CIA) risks.	♦ ♦ ♦				
Supplier Assessment (CSSA)					
The identified target security factors used in the CSSA tool are appropriate for rating the security of cloud suppliers.	♦	♦ ♦			
The result of the CSSA improves your understanding of potential cloud risks.	♦ ♦	♦			
Quantitative risk analysis (CQRA)					
The process of estimating the risk factors (impact, probability etc.) helps to limit expert subjectivity.	♦ ♦	♦			
The risk formula and resulting risk value is a good representation of cloud risk.	♦	♦ ♦			
The Monte Carlo risk calculation process is easy to understand	♦	♦ ♦			
Overall CSCCRA model					
Understandability					
The steps of the model are easy to understand	♦	♦ ♦			
The assessment guidelines and documentation are understandable	♦	♦ ♦			
Ease of Use					
The model is easy to use	♦	♦ ♦			
Usefulness and Practicality					
The model is useful for assessing cloud risks.	♦ ♦	♦			
The model's approach to addressing cloud risk is practical for use in the cloud industry.	♦ ♦ ♦				
The result of the risk assessment is reproducible and verifiable.	♦ ♦		♦		
The result of the model helps with decision-making and the implementation of mitigation.	♦ ♦	♦			

Figure 7.4: CSP-A Participant feedback on the CSCCRA model

mapping on stakeholder estimations. According to Beatson [36], protecting an organisation from supplier slip-ups means taking a big picture view of the information architecture of the cloud service and its underlying infrastructure. This level of transparency is one area where the CSCM and CSSA components of the model, provided valuable input into the risk assessment process. Another advantage of the CSCCRA methodology is that it demands visibility into the vulnerability of the chain and elicits information sharing, which is key to conducting a comprehensive RA. Likewise, the risk values calculated from the expert's estimations showed that the application of quantitative simulation to reasoned risk factor estimates made by adequately calibrated experts, combined with appropriately communicated assumptions is capable of producing meaningful risk values.

7.2 Case Organisation Two- CSP-B

7.2.1 Background of CSP-B

For confidentiality reasons, we use the name CSP-B to refer to the second case organisation. CSP-B is a small-sized security consultancy company in the south-west region of England. The company was established within the past decade and has a staff strength of about 10 to 50 employees. CSP-B consults for Large Private and Government organisations, globally delivering business improvement through the application of a comprehensive approach to advanced IT: including strategy development, architecture definition and change management. In 2018, CSP-B found a typical challenge with most of their customers around asset management and developed an asset tracking software to address this need. Built as a SaaS application, the asset tracking application is used by organisations to remotely manage the inventory of their PCs, servers, network and internet-of-things (IoT) devices. Using similar criteria to [103, 261], CSP-B estimates the market value of their SaaS application to be about £2 million. They responded to our case study invitation, which was sent through the Cloud Industry Forum (CIF) and sought to use the model to assess the security of their SaaS application.

We completed this case study on the 26th of February, 2019. Before then, we had an initial meeting with the CEO of the organisation, to brief him on our study and to highlight the benefits of using our model to assess their cloud risks. Through our discussion, we learnt that CSP-B had earlier tried to assess the risks of the application using the traditional ISO/IEC 27001 approach, but were not confident of the results. In their words, *"we needed more than a compliance stamp and desire a more comprehensive approach to assure the quality and integrity of our SaaS solution"*. The inclusive supply chain approach of the CSCCRA model appealed to the CEO, and he gave us the opportunity to trial our model on their application. In the following section, we describe the activities of the risk assessment exercise and the result of the assessment.

7.2.2 Application of CSCCRA to CSP-B-SaaS

Considering the nature of the business and the limited workforce, only two participants took part in the risk assessment exercise; the chief executive officer (CEO) who also doubled as the chief technology officer (CTO) and the lead developer of the application. Both participants, who have a combined industry experience of about 45 years, were engaged through the different stages of the assessment and provided useful anecdotes to support their design decisions and risk estimations (see Table 7.7).

In establishing the context of this assessment, we identified the asset (remote tracking application) also referred to as CSP-B-SaaS, established its value to the business, its

criticality, legal & regulatory requirements, and the operational and business importance of availability, confidentiality and integrity. The participants identified the application as their core revenue-generating system and prioritised the integrity of CSP-B-SaaS over its confidentiality and availability requirement.

CSCCRA is a business-aware cloud risk assessment model, which accounts for the role IT infrastructure and third parties play in a risk scenario. So before identifying the vulnerabilities of CSP-B-SaaS or the threats it is exposed to, we carried out the model's pre-assessment activities, i.e. supply chain mapping and supplier security posture assessment. This process provides us with a high-level or initial assessment of the cloud service and gives us an insight into its scope and weaknesses. According to Gaonkar & Viswanadham [114], to manage the uncertainties in the supply chain, stakeholders should identify the exceptions that can occur in the chain, estimate the probabilities of their occurrence, map out the chain of possible adverse events and quantify their impact. All of this functionality is incorporated into the CSCCRA model, and in the following sections, we will follow the steps listed below to assess the risk of CSP-B-SaaS.

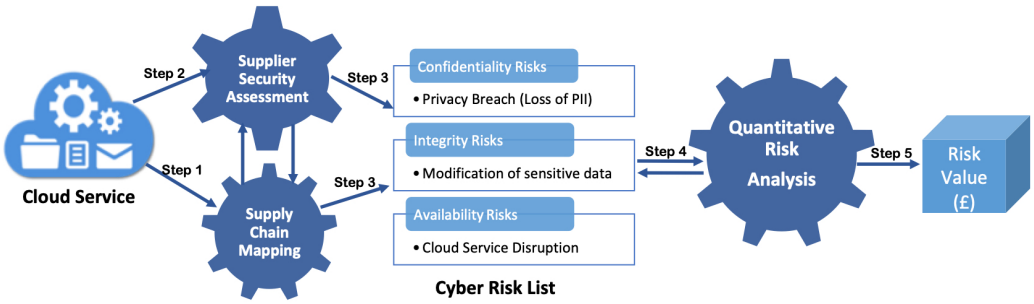


Figure 7.5: The CSCCRA Model steps for assessing CSP-B risks

1. Decompose the cloud application into its component services and map out the supply chain.

2. Assess the security of the supplier of each service component using a multi-criteria decision support system.

3. Identify the weak link(s) within the chain and compile a comprehensive list of cloud security risks.

4. Enable stakeholders within the CSP to make reasonable estimates of risk values.

5. Input risk values to the CSCCRA quantitative simulation tool to arrive at the risk value in monetary terms.

Table 7.7: List of Participants for Case Study Two

No.	Stakeholder	Role	Extent of Participation
1.	Participant-B1	CEO/CTO	Participated in all phases of the study
2.	Participant-B2	Lead Developer	Participated in all phases of the study

Table 7.8: CSP-B First-tier Supplier list

Anonymised Supplier	Component	Service Category	System Criticality	Data Proce-using (Y/N)	Data Stora-ge (Y/N)
SD-Pro-B	Service Desk	Application	Not Critical	Y	Y
CSP-B	*SaaS Integration/ Software development*	*Application/ Platform*	*Critical*	*Y*	*Y*
Code-Repo-Pro-B	Code Repository	Application	Not Critical	N	Y
PAM-Pro-B	Privileged access management	Application	Critical	Y	N
IaaS-Pro-B	Database, IaaS, DNS, Backups	Infrastructure/ Application	Very Critical	Y	Y
AD-SaaS-Pr-B	Active Directory	Application	Critical	N	Y
IAM-Pro-B	Identity Management	Application	Very Critical	Y	N
Perf-Mon-Pro-B	Application Performance Management	Application	Not Critical	Y	Y
MFA-Pro-B	Multi-Factor Authentication	Application	Critical	Y	N
Log-Pro-B	Log Management	Application	Not Critical	Y	Y

7.2.2.1 Supply Chain Mapping

In complying with our assessment framework, we decompose CSP-B-SaaS into its component services, while also identifying their suppliers. This step began with a data flow diagram (DFD) provided to us by the CSP to illustrate the flow of traffic through the asset tracking SaaS. In the DFD, details of the individual components, their function and supplier was identified. Seeing that the importance of the CSCM tool is to provide a visual structure that illustrates the interdependencies between the components and highlights relevant information that enables CSPs to recognise the risk in critical but lower-tier suppliers, we sought to improve on the DFD. We leveraged technology lookup websites such as builtwith.com [52] and Google to gather additional data on the lower tiers of the supply chain, identifying the infrastructure hosting, DNS and IAM providers for some of the components. The resulting map (see Figure 7.8) provides a comprehensive view of the supply chain, which assists CSP-B in assessing the criticality, threat and vulnerabilities of their direct and indirect suppliers. This process also ensures that comprehensive information on the supply chain is transparent to stakeholders during the supplier assessment and risk analysis phase.

In assessing the criticality of the suppliers, the researcher (risk assessor) applied the

action research method, using a whiteboard session to engage the participants in a discussion as to which of the components, CSP-B-SaaS required to function, even at a minimal level. We experimented with various"what-if" scenarios to arrive at the result presented in Table 7.8.

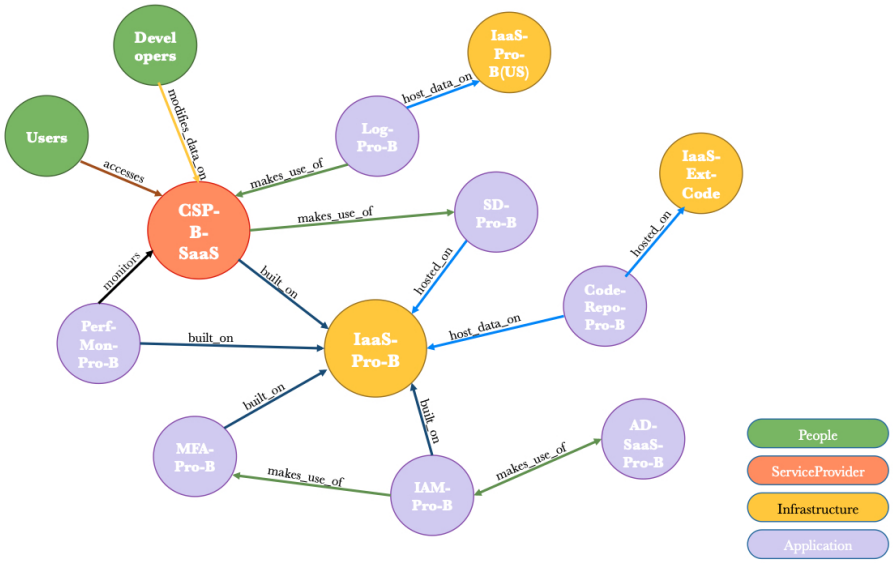


Figure 7.6: Supply Chain mapping of CSP-B-SaaS using the CSCM tool

Figure 7.6 provides a visualisation of CSP-B-SaaS supply chain and identifies single points of failures (SPOFs) within the chain. One of the suppliers that immediately stands out is IaaS-Pro-B, the infrastructure provider for CSP-B, who also provides infrastructure and/or hosts data for all other suppliers involved in the delivery of CSP-B-SaaS. Both participants were surprised by this observation since they had not paid close attention to the lower tiers of their supply chain; a strength of the CSCCRA approach. The map highlighted the criticality of the infrastructure provider and the total dependence of the SaaS application on IaaS-Pro-B. While IaaS-Pro-B represents a SPOF for multiple components of the cloud service, the participants were somewhat comforted by the fact that it is one of the "Big Four" cloud providers and has an excellent industry reputation for security and redundancy.

The supply chain map helps with the provenance (traceability) of a cloud service, maintaining an end-to-end record of the entities involved in the delivery of the service to some degree of abstraction. Providing end-to-end supply chain visualisation enables organisations to identify their areas of weakness, strengths and the potential risks to their service while also supporting collaboration and decision-making within the chain [293]. Another interesting observation from the map was that the log provider (Log-Pro-B) primarily hosted customer data in a United States (US) datacentre owned by IaaS-Pro-B. Although the participants were aware that IaaS-Pro-B was the 2nd tier provider for Log-Pro-B, they were

not aware that by default, all log data was sent to the US. This information led to a conversation around legal jurisdiction and data protection (GDPR), one which CSP-B promised to resolve or inform customers.

In summary, we see from this study that the use of mapping tools to illustrate the interdependencies between the components helps to visualise the cloud information flow and promotes transparency, thereby assisting CSPs to implement controls proactively.

7.2.2.2 Supplier Security Assessment

In this section, we appraise the security posture of the SaaS application's supply chain, to identify suppliers who based on their lack of transparency or limited security control implementation, could be referred to as weak links, i.e. those with the highest susceptibility to a cyber attack.

The CSSA tool builds on the visual structure of the SaaS's supply chain and presents CSPs with a consistent approach to assessing and comparing their suppliers based on our nine (9) security target dimensions (see below). It facilitates the conduct of comprehensive due diligence on the security controls of the CSP's suppliers. Assessing the security processes of suppliers makes the stakeholders investigate their supplier controls such as personal data encryption, data breaches detection & communication, data storage and location, and how supplier's use of sub-processors impact these controls. This assessment also helps with GDPR compliance [283], to proactively identify personal data processing suppliers that will be accountable to the ICO and data subjects, in the event of a data breach [198].

1. Availability of Service (AoS)
2. Data & System Hosting (DSH)
3. Data Security Controls (DSC)
4. Maturity of Security Assessment process (MSA)
5. Maturity of Operational Security (MOS)
6. Security Governance and Compliance (SGC)
7. Identity and Access Management (IAM)
8. Encryption & Key Management (EKM)
9. Application Security (AS)

Table 7.9: Assessing CSP-B Suppliers using CSSA

Anonymised Supplier	**AoS**	**DSH**	**DSC**	**MSA**	**MOS**	**SGC**	**IAM**	**EKM**	**AS**	**Combined Z-Score Value**
SD-Pro-B	9	9	7	9	10	10	9	8	9	-0.43
CSP-B	*8*	*7*	*8*	*8*	8	*5*	*9*	*8*	*6*	*0.63*
Code-Repo-Pro-B	8	9	9	10	9	9	9	8	9	-0.34
IaaS-Pro-B	9	9	9	9	8	10	10	9	8	-0.69
AD-SaaS-Pro-B	9	9	9	9	9	10	10	9	8	-0.78
IAM-Pro-B	8	6	7	10	9	10	10	9	9	-0.25
Perf-Mon-Pro-B	9	9	5	7	6	7	7	8	3	1.02
MFA-Pro-B	8	8	8	7	7	7	9	9	6	0.39
Log-Pro-B	8	9	8	8	7	7	8	8	7	0.46

We began this phase of the case study by finding out how much CSP-B knew about each of the identified suppliers. As we talked through each of the security factors, we gauged that the provider had a sufficient level of information on their suppliers, and have done their due diligence. While CSP-B prioritised security, they also applied similar criteria to CSP-A in selecting vendors including price, functionality, industry reputation and past working knowledge.

In assessing the security of the suppliers, we informed the participants to consult the supplier website, SLA documents and online searches before scoring each supplier. To enhance the objectivity of the participants scoring, we also referred to the CSA's STAR Registry, to find out which of the suppliers have completed the Consensus Assessments Initiative Questionnaire (CAIQ). The CAIQ is a due diligence questionnaire that allows CSPs to demonstrate their compliance to potential customers through the documentation of their implemented security controls [58]. This document could provide us with the information needed to assess some of the supplier security controls. However, of the eight (8) suppliers identified for CSP-B-SaaS, four (4) had an entry in the registry, but only two were current(i.e. 2018/2019). The other two were dated 2012 and 2014 respectively. This did not come as a surprise, seeing that only about 350 cloud vendors have completed the assessment out of the thousands of CSP around the world [75]. Table 7.9 presents the participants' assessment of each supplier's security posture.

As shown in Table 7.9, Perf-Mon-Pro-B was judged to be the weakest link in this supply chain, followed by CSP-B themselves and Log-Pro-B. For the performance monitoring provider (Perf-Mon-Pro-B), the stakeholders scored them low on data security controls (DSC) and application security (AS), because they provided limited information on their website on the implemented controls that assure these factors. Although they provided more information on their CAIQ self-assessment, much of the information was referencing the controls in place at their hosting provider (IaaS-Pro-B). Likewise, Perf-Mon-Pro-B

scored the lowest score for AS, and this was due to the basic level of protection they had in place for virtual machines and the limited information on their coding practices, which they claim to be proprietary. CSP-B, despite their detailed and secure architecture, scored low in security governance and compliance (SGC), due to their reliance on suppliers for the compliance of their service. Also, the supplier assessment showed that CSP-B needed to improve their application security and SDLC processes. The participants confirmed that they lacked processes around comprehensive security testing and release management.

Furthermore, Log-Pr-B who is an ELK Stack (Elasticsearch, Logstash and Kibana) provider, scored low on the maturity of their operation security (MoS) because of the limited information around DR/BCP, change control and data breach handling. Going by the lessons learned in case study one, participants were advised to score suppliers low where they found no information on supplier processes. We interpret the lack of information to mean that participants could not determine if supplier practices aligned with that of CSP-B or confirm the nature of the risk inherited by their integration. Through our search, we found suppliers who confirmed not to have an organisation-wide risk management structure, who encrypted all tenant on a single SaaS cluster with the same encryption key and did not have proper segregation of tenant's data. Some other suppliers had traditional security measures in place, which in the face of changing risk landscape and growing sophistication of attackers, was judged insufficient.

On a positive note, the participant assessed the security posture of suppliers such as IaaS-Pro-B and AD-SaaS-Pro-B to be the most secure in comparison to the rest of the chain. A commonality between the two providers lies in the size of their global operation, the comprehensiveness of their security processes and the full range of their customers. Also, the fact that most of CSP-B's suppliers relied on IaaS-Pro-B reinforces the trust the cloud industry has in the supplier. This trust, which is based on the knowledge of IaaS-Pro-B's processes, architectures, compliance and visible controls, places them as one of the de facto providers. In the course of the assessment, CSP-B also found out about security features provided by some other suppliers which they were not leveraging. Controls such as MFA for the admin panel, encrypted backup, geographic retention of data and access to audit data. Another interesting observation was the availability of transparency reports on the website of two of the suppliers, which detailed Governments' request for data.

Overall, we believe that the supplier assessment was worthwhile to the CSP and the participants. The search through online resources and in-house documentation for supplier controls and processes, and the discussion that ensued after a new feature was found showed that the supplier assessment was beneficial to the CSP-B-SaaS platform. The ability of such activity to influence and improve the design of the cloud service also fulfilled one of the purposes of the assessment from the CSP's perspective.

7.2.2.3 Quantitative Risk Analysis

Recognising that the objective of a risk assessment is to understand the existing system and environment, and identify risks through analysis of the information/data collected, the structured approach of the CSCCRA model provided the participants with a 'big picture' of the CSP-B-SaaS application.

In this phase, the participants built on the results of the supply chain mapping and supplier security assessment, to identify the weak areas the SaaS platform and identify relevant vulnerabilities, threats and probable risk events. Before beginning, we gave the participants a presentation on quantitative risk analysis and risk estimations, after which we presented them with a short calibration exercise. We informed the participants of the need to provide their estimates to a 90% CI. Participant-B1, had three of the six questions estimated correctly while Participant-B2 only managed one. This information, together with the specificity of the expert's role, and the level of knowledge displayed during the assessment, was considered when we combined the expert risk factor estimates.

Through the risk identification stage, we reminded the participants to ensure that the identified threat can exploit a vulnerability of the system or organisational processes; otherwise, it is not a risk. With our participants experienced in the complexities of the systems, processes and cost implications, we tasked them with identifying the risks of CSP-B-SaaS based on its business operations and extended supply chain. According to Schmitting [274], some of the organisational value derived from conducting a risk assessment exercise include identifying the organisation's most significant risks, evaluating them, reaching a consensus on steps to mitigate the risk and communicating the findings to senior executives. We followed this disciplined and structured approach to improve the objectivity of CSP-B's analysis.

Being a critical application for the organisation with a global customer base, CSP-B prioritised the integrity of the application over its confidentiality and availability. Using a threat, vulnerability, and asset taxonomy that complies with ENISA's method of structuring risk information [58, 196], we presented the participants with a spreadsheet to list the risks. The spreadsheet was populated with possible vulnerabilities, threats agents, threat types and security effect. This approach was based on the feedback of the first case study. Participants were also allowed to add new risk factors as the situation demanded. At the end of the exercise, the participants identified and tracked the top 10 risks of CSP-B-SaaS in the risk register (see Table 7.10). The visualisation aided the participants in identifying potential supply chain risks, particularly those for which they have no processes or controls in place to manage.

Together with the participants, we identified the existing controls (safeguards and countermeasures) CSP-B has in place to address the identified risk. This was done to provide

the participants with a comprehensive picture of the risk to enable them to estimate the value of the risk factors objectively.

Uncertainty is inherent in the evaluation of risk, due to the imperfect or incomplete knowledge of the threat, the ever-increasing discovery of vulnerabilities and the unrecognised dependencies that can lead to unforeseen impacts [258]. Therefore, for each risk item, the CSCCRA model expresses the participants' degree of uncertainty quantitatively using probability distributions. Also, to avoid a bias in the risk analysis stage, the CSCCRA uses a combination of the NIST's vulnerability-oriented and asset/impact approaches [258]. Each participant provides us with an independent estimation of the probability of the risk event, frequency and impact cost to a 90% confidence interval. Due to the insufficient quality data points and data sharing in the cloud industry, the participants were encouraged to be resourceful and objective and to make use of the results of our pre-assessment activity in their estimations. Acknowledging our inability to eliminate risks, we settle for pragmatically reducing uncertainty around risk events and having enough information to mitigate the top risks.

Table 7.11 presents the combined participant estimates for each of the risk items. The estimates for the probability of risk occurrence (with or without control) and impact were presented in a PERT probability distribution format, including the LB, ML and UB estimates, while that of frequency was based on an average rate of occurrence.

Our observation of the participants' estimation of risk factor values, showed the multi-dimensional aspects of risk assessment and how the CSCCRA could assist stakeholders in reducing the cognitive bias. For instance, in estimating a risk item, we saw participants consider the reputational risks, the cloud components involved and the interaction between the risk factors. Similar to case study one, an aspect of the risk evaluation which participants found difficult was the estimation of impact, seeing that it grows exponentially with the size of the underlying system, utility, complexity and most importantly time [261]. However, a lesson the researcher learnt from this exercise (provided by Participant-B1), was that in such estimations, it was important for experts to have a reference point (e.g. the value of the product, cost of replacement, and fines). This process increases the objectivity of risk estimations and helps participants compare risk scenarios and assess the effectiveness of countermeasures.

On completing the estimations, the researcher gathered the data and analysed each risk item using our Monte Carlo simulation-based, CQRA tool. Since each participant's perception is different, the risk factor estimate was based on their confidence level (under/over) [53]. We chose the Monte Carlo method to help us arrive at an optimal decision based on the decrease in the degree of uncertainty, with participants providing their estimates as a

Table 7.10: List of Security Risks identified by the CSP-B Stakeholders

Risk No	Risk Description	Asset at Risk	Supplier	Vulnerability Name	Threat Agent	Threat Type	Security Effect	Existing Controls
R1.	Disgruntled employee disrupts CSP-B-SaaS by polluting or corrupting critcal data	Database, Source code	IaaS-B-Pro, CSP-B	Application/Platform vulnerability, System or OS vulnerabilities, Unclear roles and responsibilities, Poor integrity or backup controls	Privileged Insider	Sabotage, Data Loss/Manipulation, Website defacement	Integrity, Availability	Backup, privileged management (PAM), Logging, HR Termination process & Employment screening
R2.	Accidental misconfiguration of access control exposes CSP-B-SaaS data	Customer PII in DB and AD, Intellectual Property (IP)	CSP-B, Code-Repo-Pro-B, IaaS-Pro-B	Insufficient IAM controls, Poor key management, Weak encryption, Non-optimal change control, Unavailable or misconfigured security controls, shared platform vulnerabilities	Accidental Insider	Information/Data leakage, Service outage, Data Loss /Manipulation, Loss of governance	Confidentiality, Integrity	Backup, Logging, Awareness and Training, Penetration testing
R3.	Malicious/accidental attack of privileged access control locks out CSP-B-SaaS Admin	Privileged Access Management	PAM-Pr-B, CSP-B	Application/platform vulnerability, Failure of configuration management, system or OS vulnerabilities	Accidental Insider, Malicious Outsider, Privileged Insider	Sabotage, Lock-in, Loss of governance	Availability	Penetration testing, MFA, Backup, Code repository
R4.	Compromise of IAM-Pro-B facility to obtain privileged access to CSP-B-SaaS	Identity & Access Mgmt, Database	IAM-Pro-B, CSP-B	Insufficient IAM controls, shared platform vulnerabilities, Weak authentication mechanism, Insiders on provider side, hidden application dependency	Malicious Outsider, Political	Malicious Probes or scans, Cross-site scripting, Social Engineering, Management interface compromise, Lock-in	Confidentiality, Integrity, Availability	MFA, Third party supplier selection, Logging
R5.	Malicious outsider inserting malware into CSP-B-SaaS code repository	Code repository (IP)	Code-Repo-Pro-B, CSP-B	Insufficient IAM controls, Failure of configuration Mgmt, shared platform vulnerabilities, Unavailable or misconfigured security controls, lack of monitoring mechanism	Malicious Outsider	Sabotage, Data Loss/ Manipulation, Loss of governance	Integrity, Availability	Change (+release) process, code scanning
R6.	Non targeted DDoS attack affecting Asset tracking SaaS	CSP-B-SaaS (front -end, Database)	CSP-B, IaaS-Pro-B	Inadequate resource provisioning, Limited redundancy, multi-tenancy, Bandwidth under-provisioning, Lack of resource isolation, Lack of supplier redundancy	Malicious Outsider, Political , Environmental	Malicious Probes or scans, Denial of Service, Fraudulent resource consumption attack	Availability	N/A (rely on supplier controls)
R7.	Loss of customer PII due to inadequate security controls	Service Desk, Database, Active Directory	Service-Desk-Pro-B, IaaS-Pro-B, AD-SaaS-Pro-B, CSP-B	Insufficient IAM controls, Weak encryption, Non-optimal change control, weak physical security measures, Unclear roles& responsibilities	Malicious Outsider, Privileged Insider	Information/Data leakage, Social Engineering, Brute force and Dictionary attacks, Data Loss/Manipulation, Loss of governance	Confidentiality	PAM, MFA, Logging
R8.	Service outage due to vendor supply chain failure affecting CSP-B-SaaS	AD, Database, IAM, CSP-B web fronted	AD-SaaS-Pro-B, IAM-Pro-B, CSP-B	limited redundancy, system or OS vulnerabilities, Poor provider selection, Lack of supplier redundancy, hidden application dependency	Environmental, Accidental Insider	Service outage, Supply chain failure	Availability	Supplier Selection
R9.	Data breach of customer PII data	Database, Active Directory	AD-SaaS-Pro-B, IAM-Pro-B, CSP-B	Insufficient IAM controls, Failure of configuration management, Unavailable or misconfigured security controls, insecure systems database	Privileged Insider	Information/Data leakage, Data Loss/Manipulation, Supply chain failure	Confidentiality, Reputation	Encryption, PAM, Incident management, Logging (SIEM)
R10	Leakage of admin credentials including second factor	IAM, PAM	CSP-B, IAM-Pro-B, MFA-Pro-B	weak physical security measures, Training and awareness	Malicious Outsider, Insiders	Non-compliance, Abuse and Nefarious use of cloud service, Data Loss/Manipulation, Information/Data leakage	Confidentiality, Reputation	Least Privilege, RBAC

Table 7.11: CSP-B Risk Analysis result based on CQRA calculation

Risk No	Probability of occurrence (without control)			Probability of occurrence (with control)			Impact Cost Estimate (£)			Frequency (per year)	Risk Value (£) Estimates (without controls)			Risk Value (£) Estimates (with controls)			Estimated Risk Value (£) based on Existing Controls
	LB	ML	UB	LB	ML	UB	LB	ML	UB		LB	ML	UB	LB	ML	UB	
R1.	3.80%	11.03%	23.86%	2.59%	5.17%	9.00%	£15,302	£253,983	£851,634	0.71	£0	£20,886	£106,280	£0	£9,418	£49,920	**£36,357**
R2.	6.12%	11.79%	19.01%	3.44%	6.07%	9.87%	£4,835	£35,126	£78,186	0.23	£0	£1,001	£6,531	£0	£524	£3,362	**£2,039**
R3.	1.33%	4.35%	7.39%	1.37%	2.57%	3.95%	£857	£7,396	£20,711	0.08	£0	£25.80	£146	£0	£15	£90	**£90**
R4.	3.00%	7.31%	12.36%	2.01%	4.30%	7.05%	£41,352	£390,737	£996,566	0.05	£0	£1,628	£3,190	£0	£990	£2,108	**£2,108**
R5.	5.50%	10.44%	15.66%	1.79%	3.64%	6.83%	£23,800	£273,549	£807,160	0.06	£0	£1,628	£5,031	£0	£592	£1,547	**£1,627**
R6.	3.87%	8.35%	12.72%	2.62%	7.90%	12.73%	£276	£4,408	£14,538	0.35	£0	£130	£778	£0	£123	£725	**£778**
R7.	6.12%	10.24%	15.11%	2.85%	5.20%	7.84%	£12,005	£131,769	£623,029	0.17	£0	£2,322	£7,425	£0	£1,142	£3,952	**£1,667**
R8.	5.53%	10.71%	16.59%	5.53%	10.70%	16.57%	£1,745	£8,836	£19,534	0.23	£0	£225.57	£1,306	£0	£223	£1,290	**£1,306**
R9.	6.08%	10.26%	15.39%	2.79%	5.47%	8.76%	£12,102	£133,538	£625,461	0.17	£0	£2,330	£8,511	£0	£1,236	£4,549	**£4,549**
R10.	2.98%	5.32%	7.93%	2.01%	4.49%	7.60%	£8,996	£115,823	£323,703	0.08	£0	£524	£3,212	£0	£445	£2,535	**£3,211**

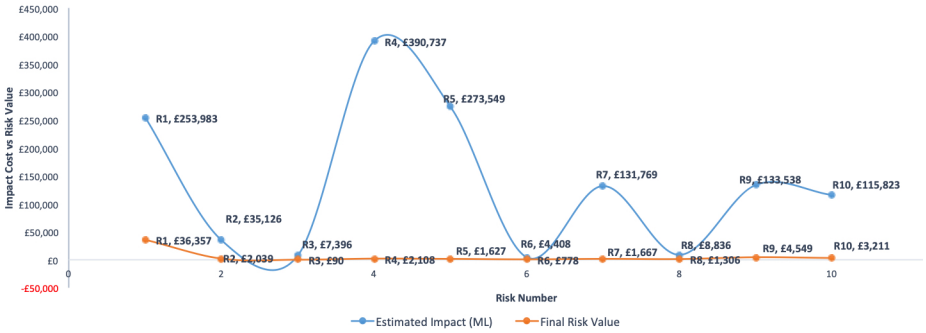


Figure 7.7: CSP-B's Impact Estimate vs. Risk Value Calculation

probability distribution. We follow the example of the risk calculation carried out in section 6.3 to build models of possible risk results based on the estimations of the risk factors. Each risk result was calculated over five (5) simulations of a hundred thousand (100,000) iterations each, producing a distribution of possible risk values for a particular risk item. At the end of the simulation, we applied a mental litmus test to verify that the result of the CQRA simulation is in line with the estimations of the participants.

As shown in Table 7.11, we calculated two sets of risk values, one with controls and the other without controls, based on the probability estimates for each scenario. This risk value calculation then informs our estimated risk value based on existing controls. For this case study, the estimated value of each risk item ranged from £90 to £36,357, which represents between 65% to 95% percentile of the risk value continuum. Although CSP-B implemented quality security controls for several aspects of their service, they had oversights in a few, and in such cases, our final estimate referenced the higher range of the risk value. That said, we rounded up the values of risk R1 to R10 for ease of presentation and analysis. Figure 7.7 also shows the relationship between CSP-B's combined impact estimates (ML) and the estimated risk value, and confirms the sensitivity of the CSCCRA model to the frequency risk factor.

7.2.3 Analysis and Discussion of Assessment results

To recap the case data, the study set out to assess the risks of CSP-B's asset tracking SaaS and to assure the quality and integrity of the solution. CSP-B chose to trial the CSCCRA model after attempting to assess the risk of the platform using the ISO/IEC 27001 ISMS approach but found it inadequate. Due to the increased external interactions that expand the complexity of CSP-B-SaaS's architecture, the risk assessment process had to look beyond the focal CSP. The supply-chain inclusive approach of the CSCCRA model presented CSP-B with the opportunity to audit their security controls, including the traceability of the component suppliers and verification of their security process.

The assessment was broken into three phases: (i) supplier identification and supply chain mapping; (ii) supplier security posture assessment; (iii) risk identification and analysis. We began the assessment, first by establishing the logical and physical dependencies of the CSP-B-SaaS application. This confirmed the absolute reliance of CSP-B on IaaS-Pro-B for the delivery of the cloud service. While using the CSSA tool to assess the cybersecurity posture and conduct comprehensive due diligence on all the suppliers, we observed how the participants fundamentally questioned and rethought their established interpretations of the cloud service's security and their design strategies. This was a rationale for this study, and the result validates the applicability of the model to cloud provider environments.

Going through the list of identified risks (Table 7.10) and the participants' estimate of the risk values (Table 7.11), we can confirm the priority the stakeholders' placed on the integrity of the SaaS application. From the researcher's discussion with the participants, we understand that their most rated threat to the application lies with privileged insiders. Being a small firm with a limited workforce, where one person carries out more than one role, there is a high likelihood of people having elevated privileges than is needed for their job function. Risk **R1**, which has the highest monetary value (£36,357), depicts the impact a disgruntled employee could have on the integrity and availability of the SaaS application.

While we commend CSP-B for being proactive with the implementation of privileged access management (PAM), the risk of an insider cannot be eliminated, because it is challenging to implement zero-trust privileges within a small setting. Nevertheless, we recommend that the PAM solution is extended to access requests from the supply chain, including customers, machines, services and APIs. Two other risks which could involve an insider were also ranked second and third in the estimated risk value. For Risks **R9** & **R10**, participant-B2 had the upper bound impact cost at £2,000,000 & £1,000,000 respectively, but due to the low estimates for the probability of occurrence and frequency, the final risk value was reduced.

The assessment of CSP-B-SaaS's risk also brought to the fore the CSP's inadequate security controls for the integrated supply chain components. For instance, concerning Risks **R6 & R8**, the CSP had always relied on their third parties to have controls in place, without looking into redundancy solutions or implementing preventive controls. Seeing that we followed a scenario-based approach in the identification of risk and determination of cost-effective security controls to mitigate them, one unanticipated risk scenario was Risk **R3**. Although it turned out to be the lowest-ranked risk according to monetary value, it highlights the importance of our approach. Based on the role of the PAM, a malicious attack on the PAM application, which happens to be a virtual machine installation on IaaS-Pro-B could lock administrators and customers out of the SaaS application. In our discussion, the participants realised they had no fail-safe mechanism in place and promised to re-visit

their architecture. Furthermore, with risks involving data loss and breaches **(R7 & R9)**, CSP-B realised the need to logically segment and encrypt customer data such that the impact on a single tenant would not affect others. Some of the other areas where the need for improvement was identified include privileged access management among supply chain members, secure admin environment, proactive logging and monitoring, supplier and data redundancy, encryption and key management, secure backup, data classification, integrity checks and management of code repository.

The empirical findings from this study confirm that our proposed model addresses the efficiency and statistical robustness challenge synonymous with quantitative models [261]. However, one area we identify a need for improvement is the reliable valuation of asset and impact cost. Despite providing participants with a list of criteria to consider when estimating risk factors, some of their estimations seem to suggest extreme subjectivity. For example, Participant-B1's upper bound impact estimate for Risks **R5 & R7** suggested that CSP-B will be out of business should the event happen. We do not believe this is accurate, considering their existing controls. However, seeing that the company's value is built on consumer trust, it is not totally out of place. Also, with GDPR fines costing up to 20,000,000 euros, one can understand from a business perspective why a CEO will be extremely worried about the loss of customer PII data or a malicious attack on their code repository. Although we prefer to have participants estimate each risk factor accurately, we realise that it costs exponentially more to reach this level of accuracy. Valuable information such as the cloud industry's data on security incident/risk required to improve on participants estimations is often held back by the security companies due to proprietary competitive advantage [184, 261].

7.2.3.1 Risk Mitigation and Treatment Recommendation

In this section, we present security controls that could mitigate or limit the impact of the assessed risks and improve CSP-B's security posture. According to Jones [162], security controls can be characterised through three dimensions: forms (policy, process, or technology), purpose (preventive, detective, or responsive) and categories (loss event, threat event and vulnerability). We have attempted to address each one of these dimensions in the suggested list of best practices in Table 7.12. We consulted cloud security best practice documentations [98, 267] and other standards and guidance documents to identify any known control measures that would mitigate or reduce the impact of the risks.

Table 7.12 shows a list of the risks arranged in the order of their monetary value, the CSP's existing controls and our best practice suggestions. We also created an opportunity for the CSP to determine their risk treatment option and identify a risk owner. While there are four standard risk treatment options (avoid, accept, transfer, mitigate) available, our

impression is that CSP-B is likely to mitigate most of the identified risks and accept those they cannot mitigate. That said, with the growth of the cloud insurance market and the uncertainty around cloud risks in the supply chain [325], we would not rule out CSP-B taking up an insurance contract (risk transfer) to reduce liability.

Table 7.12: Treating CSP-B's identified risks based on Best Practice and assigning Risk Owners

No	Risk	Risk Description	Existing Controls	Security Best Practice	Estimated Risk Cost	Risk Treatment?	Risk Owner?
1.	R1	Disgruntled employee disrupts CSP-B-SaaS by polluting or corrupting critcal data	Backup, privileged management (PAM), Logging, HR Termination process & Employment screening	Data classification and protection, Dual control, Implement data integrity check, Data duplication, User behavior analytics, Log privileged access.	**£36,357**		
2.	R9	Data Breach of customer PII data	Privileged Access Mgmt, Incident management, Logging (SIEM)	Anomaly detection, Implement data breach notification process, Implement DB encryption, Segregate customers' data into different instances, Anonymise data in DB	**£4,549**		
3.	R10	Leakage of admin credentials including second factor	Least Privilege, RBAC	Dual Control, Separation of duties, Maintain audit trail, Timely de-provisioning	**£3,211**		
4.	R4	Compromise of IAM-Pr-B application to obtain privileged access to CSP-B-SaaS	MFA, 3rd party supplier selection, Logging	Implement multi-factor authentication for the IAM admin panel security, Proactively assess supplier controls	**£2,108**		
5.	R2	Accidental misconfiguration of access control exposes CSP-B-SaaS data	Backup, Logging, Awareness and Training, Penetration testing	Improve operational security, External audit of processes, Peer-review changes, Regular vulnerability assessment,	**£2,039**		
6.	R7	Loss of customer PII due to inadequate security controls	Privileged Access Mgmt, Multi-Factor Auth, Logging	Improve data security process (e.g. data classification and encryption (at-rest)), Audit privileges, Cyber awareness training	**£1,667**		
7.	R5	Malicious outsider inserting malware into CSP-B-SaaS code repository	Change (+Release) process, code scanning	Conduct integrity check on code repository, Backup Code repository	**£1,627**		
8.	R8	Service outage due to vendor supply chain failure affecting CSP-B-SaaS	Supplier Selection	Redundancy(supplier /technology), Proactive assessment and monitoring of critical suppliers	**£1,306**		
9.	R6	Non targeted DDoS attack affecting Asset tracking SaaS	N/A (rely on supplier controls)	Supplier redundancy, Implement provider-based DDoS solution, Web application firewall, Correctly size the web servers	**£778**		
10.	R3	Malicious/accidental attack of privileged access manager locks out CSP-B-SaaS Admin	Penetration testing, MFA, Backup, Code repository	Have a fail-safe mechanism for access to SaaS application (emergency access)	**£90**		

7.2.4 CSP-B Evaluation of Model and Case Study Exercise

In concluding the case study, we got the two stakeholders who participated in the risk assessment of CSP-B-SaaS to evaluate the CSCCRA model. Presenting them with a set of questions on a five-point Likert scale, we asked them to rate the model on criteria such as its understandability, usefulness, ease-of-use, decision-making ability, transparency and practicality. Also, we posed to the participant nine (9) free-text questions, requesting them to identify areas where the model was strong or weak, practical and useful, and to confirm how they see themselves using the model in the future.

Overall, the feedback received from the stakeholders was positive and reassuring (see Figure 7.8). The participants were impressed with the model's ability to capture the context for the cloud application, including aspects of the system that might be overlooked in a traditional asset-based assessment. The model establishes the scope and boundary for the assessment and provides comprehensive information for the risk assessment. The participants strongly agreed/agreed with all of our statements regarding the advantages of the model and its components. The feedback also shows that the model gave the participants a deeper understanding of their cloud service and insight into the system's behaviour. Participant-B1 acknowledged the robustness and ease-of-use of the CSCCRA model. He said *"I like the fact that the model follows the ISO-27005 risk assessment steps, which is familiar to many organisations. However, the way it incorporates supply chain mapping and supplier security assessment to the process is invaluable"*.

The acceptance of the model's proposition also suggests the ongoing use of the model within the organisation. When participants were asked how they see themselves applying the model within their environment, they confirmed the application of the model to *informing security design decisions, cost/benefit analyses, conducting security due diligence on supplier security, and proactive mitigation of security risks.* They acknowledged the strengths of the model to include: *making stakeholders think much clearer about some of the underlying factors behind the products used, presenting risk in monetary terms, improved visibility of dependency risk, increased objectivity in risk estimation, and fostering continuous system improvement.* The model provides CSPs with a granular view of their attack surface, and assists with the proactive implementation of safeguards, while also promoting the continuous assessment of the SaaS's security.

One of the shortcomings of the model, as highlighted by the participants, is its lack of automation, particularly for the supply chain mapping. We hope to look into this in more detail and determine if the available open-source information on cloud products can help to automate it fully or partially. With regards to suggestions for improvement, Participant-B2 asked *if it was possible to have the system components classified into different categories,*

e.g. infrastructure, software, data and cloud resources, and assessed accordingly? We understand this is possible using system automation but also note the need to develop new criteria for assessing the security of each category, just as we did with the CSSA.

Furthermore, Participant-B1 while complimenting the model's ability to assist CSPs to think through their connectivity and dependencies, *wondered if it was possible to assign the top risks systematically, to reduce stakeholder subjectivity.* We suppose this can be improved by conducting a vulnerability assessment and penetration test to identify the potential vulnerabilities and threats to the cloud platform, before presenting the information to stakeholders to estimate the risk factors. Also, Participant-B1 suggested the need for us to *link the model to a defined control set used by cloud organisations, e.g. SANS top 20, such that it will be possible for organisations to track the impact of subsequent changes to the architecture or security controls.*

The participants' feedback validated the applicability of the model to assess SaaS CSP risks and the effectiveness of its decision-making framework. They also offered useful suggestions on how to improve the model. Overall, we believe the comprehensive risk assessment exercise was also valuable to the CSP-B and provided them with useful information to improve their cloud strategy and make better decisions.

7.2.5 Summary

The empirical findings for case organisation CSP-B support our literature findings on the inadequacy of traditional frameworks in assessing cloud risks. The study validated the applicability of our proposed model in assessing cloud risks within a CSP environment and emphasised on the need for automation in cloud risk assessment. The case study highlighted the importance of applying a systematic model to cloud risk assessment, which provides stakeholders with a comprehensive view of their cloud application. The model presented CSP-B with the opportunity to objectively audit their security controls, verify supplier security processes and identify possible risks to the platform looking both inwards and outwards to the supply chain. It was useful in the conduct of a technical security assessment of the SaaS and also influenced security design decisions.

Using the CSCCRA model, we showed how the structured and systematic application of our proposed model within a SaaS organisation yields objective and defensible results which can assist stakeholders in quantifying cloud risks, reducing uncertainty and promoting better security decisions. The risk analysis approach supports the cost-effective reduction of cloud risks, while also bridging the gap between technical and business stakeholders on issues such as the value of risk, risk appetite and the effectiveness of security controls. The CSCM provided the participants with a "bigger picture" of their supply chain and its dependencies, while the CSSA enabled the participants to verify supplier security controls in place in more

Criteria	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Supply Chain Mapping (CSCM)					
The CSCM tool is a good first step in the risk assessment process	♦♦				
Identifying and mapping your cloud supply chain enables you to visualise data flow, and assists in thinking about security (CIA) risks.	♦♦				
Supplier Assessment (CSSA)					
The identified target security factors used in the CSSA tool are appropriate for rating the security of cloud suppliers.	♦	♦			
The result of the CSSA improves your understanding of potential cloud risks.	♦♦				
Quantitative risk analysis (CQRA)					
The process of estimating the risk factors (impact, probability etc.) helps to limit expert subjectivity.	♦	♦			
The risk formula and resulting risk value is a good representation of cloud risk.	♦	♦			
The Monte Carlo risk calculation process is easy to understand	♦	♦			
Overall CSCCRA model					
Understandability					
The steps of the model are easy to understand	♦♦				
The assessment guidelines and documentation are understandable	♦♦				
Ease of Use					
The model is easy to use	♦♦				
Usefulness and Practicality					
The model is useful for assessing cloud risks.	♦♦				
The model's approach to addressing cloud risk is practical for use in the cloud industry.	♦♦				
The result of the risk assessment is reproducible and verifiable.	♦	♦			
The result of the model helps with decision-making and the implementation of mitigation.	♦♦				

Figure 7.8: CSP-B Participant feedback on the CSCCRA model

granular terms. Knowing that insufficient due diligence increases cybersecurity risk [208], the CSCCRA model improves the visibility of security control across the supply chain.

7.3 Case Organisation Three - CSP-C

7.3.1 Background of CSP-C

Due to confidentiality reasons, the third case organisation is referred to as CSP-C. CSP-C is a publisher of peer-reviewed, open-access journals and books. Their flexible approach to publishing makes the platform affordable to researchers, providing them with access to information without barriers. Founded within the last decade with a staff strength of about 10 to 50 employees located mainly in their south-east of England office, CSP-C offers three essential services to the research community, one of which is the repository platform (CSP-C-SaaS), and the focus of this case study. CSP-C-SaaS is a researcher-focused repository

which supports the dissemination of published contents and helps organisations raise their scholarly profile. It supports the storage of research data and other artefacts associated with different stages of publication (e.g. articles and preprints).

The case study was completed on the 14th of May 2019. Although, before this date, we had met with CSP-C on two separate occasions to introduce the model and begin the data gathering & pre-assessment activities. Our initial meeting with CSP-C was orchestrated by a staff of the organisation who took an interest in the research after reading our BCS article on supply chain risks [10]. The initial feedback from CSP-C showed that they were not keen on the model's probabilistic Monte Carlo approach because of the widely discussed bias against quantitative risk assessment. However, they showed interest in knowing more about their supply chain security, the monetary value of their cloud risks and identifying their security inadequacies.

Furthermore, around the time of asking, CSP-C was also looking into ISO-27001 accreditation for their organisation and saw this as an opportunity to assess their security readiness. Although to avoid misleading the CSP, we informed them of our inability to prepare them for ISO-27001 accreditation, yet we provided them with ways in which CSCCRA could be of immense value in improving the security posture of their cloud service. The merits of our approach convinced them to sign up for the case study.

Because CSP-C had not conducted any proper risk assessment either of their cloud service or organisation before now, it took more effort on our side to prepare them for the risk assessment workshop. To ease them into the process, we provided them with a questionnaire (see Appendix D), which allowed them to document the processes and security controls implemented to secure CSP-C-SaaS. The questionnaire also contained questions around their supply chain setup, components, first-tier suppliers and supplier criticality, which made it possible to map an initial version of their supply chain. In the following section, we describe the case study activities and the result of the assessment.

7.3.2 Application of CSCCRA to CSP-C-SaaS

Having a group of stakeholders (technical and business) contribute to risk assessment ensures that important aspects of the cloud service are adequately considered and included in the risk assessment process. In this case study, four (4) members of the organisation took part in the risk assessment of CSP-C-SaaS (see Table 7.13). Building on the knowledge we gathered from the assessment of CSP-A & CSP-B, and ensuring that critical stakeholders were available for the assessment, we adopted a different approach in this case study.

Our request to have the CIO (Participant-C1) and CTO (Participant-C2), both of who have in-depth knowledge of the repository platform, available for the risk assessment workshop, meant we had to reduce the time of onsite workshop from one day to half-day (4

Table 7.13: List of Participants for Case Study Three

No.	Stakeholder	Role	Extent of Participation
1.	Participant-C1	CIO	Participated in all phases of the study
2.	Participant-C2	CTO	Participated in all phases of the study
3.	Participant-C3	Project Manager	Participated in the supply chain mapping and supplier assessment
4.	Participant-C4	Application Developer	Participated in all phases of the study

hours). To make that work, we opted to complete aspects of the assessment offsite and confirm the results with CSP-C through online meetings, scheduled by the project manager (Participant-C3). We completed the supply chain mapping (step 1) and the supplier due diligence (research) aspects of step 2 offsite. The other steps of the CSCCRA assessment were done onsite, except for step 5, which was completed by the assessor (researcher) and sent to CSP-C in a report.

Step 1: Decompose the cloud application into its component services and map out the supply chain.

Step 2: Assess the security of the supplier of each service component using a multi-criteria decision support system.

Step 3: Identify the weak link(s) within the chain and compile a comprehensive list of cloud security risks.

Step 4: Enable stakeholders within the CSP to make reasonable estimates of risk values.

Step 5: Input risk values to the CSCCRA quantitative simulation tool to arrive at the risk value in monetary terms.

7.3.2.1 Supply Chain Mapping

The CSCCRA model adopts security assessment best practice, in that it encourages the risk assessor and CSP stakeholders to understand the relationships and dependencies of the system and its subsystems, before assessing its risks. This provides knowledge of how policies and standards are applied within the system and helps to understand process-specific risks. An example of such information and dependency gathering activity occurs during the cloud supply chain mapping. Figure 7.14 presents an anonymised supply chain map of CSP-C-SaaS, which identifies the various components integrated into the SaaS application including the Database, File Storage, Reference & Indexing tool, Code repository and Content Delivery Network (CDN). The map also identifies the people element of the supply chain, in this case, users, developers and CSP-C administrators.

Leveraging the technology lookup website, builtwith.com [52] and Google, we gathered first and second tier supplier information on most of the component. Presenting this map to CSP-C spurred some interesting conversation about how the SaaS application worked and the controls that were put in place to secure various aspects of the service. It became apparent to the researcher (risk assessor) that the information on how CSP-C-SaaS worked was not common knowledge within the organisation and was undocumented. For example, Participant-C4 who is the lead developer of the application, only knew about the code and hosting platform, while the CTO (Participant-C2) was in charge of its technical operation including backup, security, indexing, availability and DNS. Supply chain mapping helps with the provenance (traceability) of a cloud service and having an end-to-end picture of the entities involved in service delivery. It supports the comprehensive identification, assessment and mitigation of risks. This was the case with CSP-C, who as part of the initial discussion on the supply chain map, immediately identified some flaws in their security controls.

The supply chain mapping process aids the quick and accurate visualisation of the cloud information flow through the supply chain and helps to identify critical suppliers of the service and SPOFs within the chain. Using the CSCM tool for the pre-assessment exercise helps to define a scope and boundary for cloud assessment [151]. This is because the move to the cloud blurs the existence of physical boundaries that CSPs could proactively monitor for cyber threats.

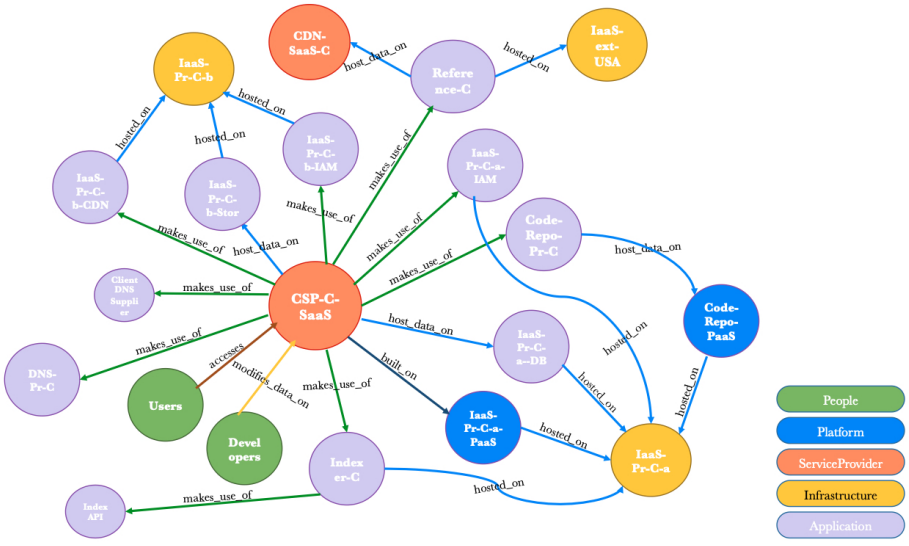


Figure 7.9: Supply Chain mapping of CSP-C-SaaS using the CSCM tool

In Figure 7.14, we see the dependency of CSP-C-SaaS on IaaS-Pr-C-a, a "Big Four" provider, who hosts the repository application and its Database. IaaS-Pr-C-a also hosts the infrastructure for the code repository service and indexing service used by CSP-C-SaaS. The number of components relying on IaaS-Pr-C-a to function makes the infrastructure provider

Table 7.14: CSP-C First-tier Supplier list

Anonymised Supplier	Component	Service Category	System Criticality	Data Proce-using (Y/N)	Data Stora-ge (Y/N)
IaaS-Pr-C-a	Hosting (Web, Code), Database & IAM	Infrastructure/ Application	Very Critical	Y	Y
IaaS-Pr-C-b	Content Delivery, File Storage, IAM	Infrastructure/ Application	Critical	Y	Y
CSP-C	*SaaS Integration/ Software development*	*Application*	*Very Critica*l	*Y*	*Y*
Code-Repo-C	Code Repository	Application	Critical	Y	Y
Indexer-C	Research Indexing	Application	Critical	Y	N
Reference-C	Research Indexing	Application	Critical	Y	N
DNS-Pr-C	DNS	Application	Very Critical	Y	Y

the most critical component of the SaaS application. CSP-C also uses another of the "Big Four" providers, IaaS-Pr-C-b, for content delivery and file storage. The observed concern with the CSP-C-SaaS setup is that, although it seems like there is IaaS supplier redundancy, the functions carried out on both principal providers are not duplicated, and an outage on one will lead to the unavailability of the service. CSP-C have also not implemented high-availability with a single provider, except where it is offered as part of the service, as is the case with the database. This, we gathered was done for cost reasons, but indicate availability concerns, seeing that the 3Rs (resiliency, reliability and recoverability) are not optimal in the CSP-C-SaaS architecture.

Furthermore, while experimenting with various "what-if" scenarios, another very critical component of this supply chain was identified to be the domain name system hosted by DNS-Pr-C (see Table 7.14). DNS is critical to the delivery of any cloud service as it hosts the domain name to IP addressing mapping of the service components. An attack on, or outage of DNS-Pr-C, which in this case is a SPOF, would lead to an outage of the cloud service. An anecdote of this was the outage of major cloud providers in 2016 when the Dyn DNS infrastructure was under a sustained DDoS attack for several hours [139].

In summary, the visibility provided by the supply chain mapping process increases the awareness of stakeholders about the potential risks of the platform and as we will see in the subsequent sections, helps during the supplier assessment and risk analysis phase.

7.3.2.2 Supplier Security Assessment

According to Chang et al. [60], the selection of appropriate suppliers is one of the most critical challenges affecting the performance of cloud services. Studies have shown that when selecting a cloud vendor, cloud stakeholders prioritise cost, service suitability, vendor reputation and functionality, over security [20]. With the cloud supply chain being a technology-enabled arrangement and in some cases dynamic, it is crucial for CSPs to

Table 7.15: Assessing CSP-C Suppliers using CSSA

Anonymised Supplier	AoS	DSH	DSC	MSA	MOS	SGC	IAM	EKM	AS	Combined Z-Score Value
IaaS-Pr-C-a	9	10	9	10	10	10	9	9	10	-0.98
IaaS-Pr-C-b	9	10	10	10	*10*	10	10	9	10	-1.21
CSP-C	*8*	*7*	*8*	*7*	*7*	*8*	*7*	*7*	*8*	*1.01*
Code-Repo-C	8	9	9	9	9	9	9	9	9	-0.35
Indexer-C	8	8	7	6	8	7	8	8	9	0.73
Reference-C	8	8	8	7	8	9	8	8	8	0.45
DNS-Pr-C	7	9	8	7	9	8	9	9	7	0.36

prioritise security by understanding the vulnerabilities of each component supplier and implementing controls to mitigate known threats.

In this section, we build on the visual structure of the CSP-C-SaaS's supply chain and evaluate the security of the component suppliers of CSP-C-SaaS. The CSSA tool presents CSPs with a consistent approach to assessing and comparing suppliers based on nine (9) security target dimensions. Conducting this comprehensive due diligence on component suppliers also helps with GDPR compliance by proactively identifying data processors and their data lifecycle controls. Using the objective and quantitative security metrics from our Delphi study [12], we assess the performance of each supplier, comparing them with each other. Assessing suppliers based on the visibility of controls and awareness of security processes means that suppliers with limited transparency or information on security control implementation, are referred to as the weak links of the supply chain.

Table 7.15 presents CSP-C-SaaS's supplier security rating based on the information available to the team (researcher and CSP stakeholders). As mentioned previously, to improve the speed of the process, the researcher conducted an initial data gathering on the security dimensions from the different supplier websites and online forums. This laid the foundation for the evaluation of each supplier's security. As was expected, some of the information uncovered about each supplier was new to the CSP. CSP-C is not fully abreast with their vendor security offerings, and in the cases where they were, they are not quick to implement the controls due to resource constraints. This would appear to be a common challenge with SMBs who manage multiple cloud environments without the correct processes in place.

Similar to CSP-A, CSP-C also rated themselves as the weakest link in the supply chain. We agree with this assessment, going by the technical security controls that can be improved on by the provider, particularly around central logging, monitoring and privileged access management. For example, MFA is offered by most of the component suppliers, but CSP-C is yet to implement this security feature on their repository platform. Privileged accounts which typically carry the highest risk and impact, are not managed appropriately, and a compromised privileged account can lead to significant permissions and access rights being

obtained and the user/attacker negatively impacting the organisation. Also, CSP-C does not have a documented recovery plan which could be crucial to recovering critical and essential operations following an outage. We observed the lack of clearly defined roles and the reliance on a single personnel resource (SPOF) for multiple critical activities, which constitute a weakness of the supply chain.

Turning now to the external suppliers, the indexing provider (Indexer-C) was judged the weakest supplier in the chain. The indexer supplier website provided no information on their security controls. CSP-C also knew less about this supplier. They scored low on the MSA security dimension, not only because of their lack of security certification but for the lack of information on a security assessment. Their website provided incomplete information around their privacy policy (DSC), availability of service (through their status page), encryption and API controls. We relied on builtwith [52] to identify the hosting provider and increase our knowledge of the supplier. Indexer-C will go down as the company with the least information on security, of all the suppliers we examined in the course of the three (3) case studies. Nevertheless, it remains an integral part of the repository platform because its unavailability will result in a degraded service.

Furthermore, the supplier, Reference-C, also makes for a good discussion. Suppliers go about security transparency with customers in different ways. Reference-C demonstrated their implementation of security controls with the SOC 2 accreditation. The SOC 2 assessment which covers five categories, namely: security, availability, confidentiality, processing integrity and privacy [296], assesses the design and operational effectiveness of the CSP's security and availability controls. However, it was not possible to confirm all the principles that were addressed in Reference-C's review and the extent of assessment. So in assessing security dimensions not explicitly covered in a SOC2 report, where also the supplier provided little or no information, the stakeholders were encouraged to give a lower score.

Also, as part of this due diligence exercise, we confirmed the current DNS provider (DNS-Pr-C) to be located in France. When asked how CSP-C came to hosting their domains with a provider in France, there was no apparent reason, and the decision appeared to have been based on cost and functionality. While considering that the DNS provider is not the weakest link, DNS-Pr-C's cloud architecture, outage history, lack of industry certification and criticality to CSP-C-SaaS raises a cause for concern. IaaS-Pr-C-a and IaaS-Pr-C-b were judged to be secure and their processes were perceived to be surplus to the requirements of the CSP. This is expected, seeing that both providers are global players, compliant with almost all industry and government standards, and their combined hosting capacity will likely account for half of the global cloud use.

In summary, one recurring advantage of the CSSA and overall CSCCRA approach is that it encourages communication among stakeholders. The time set aside for the assessment

affords busy stakeholders who ideally will not have the time to discuss and review their cloud environment with their colleagues, the opportunity to do so. According to Participant-C1, *"the discussion with (the researcher) and the team were useful. Some discussions would not happen in the same way without the exercise taking place. I am now more informed about our products and our risks"*. The participatory case study method also enables us to establish trust with the CSP, giving us access to sensitive information and critical stakeholders.

7.3.2.3 Quantitative Risk Analysis

Going by the well-defined steps of the CSCCRA model, the next phase of our assessment was to identify the top ten risks of the cloud service and estimate the risk value. Research has shown that cloud stakeholders are required to understand their risks before they can evaluate and mitigate them. The inclusion of the CSCM and CSSA tools into the risk assessment process is valuable to CSPs in that it presents them with a clear understanding of the components that make up the service and the supplier security processes that protect them.

At the start of the risk analysis phase using the CQRA tool, we reminded the participants of our three-fold proposition towards measurement: i) assume this has been measured before; ii) by being resourceful, you can find more data; iii) you need less data than you intuitively think you need [142]. We encouraged them to avoid subjective over-confidence or under-confidence, giving them examples and a short calibration exercise. Also, we provided the participants with information on how to estimate values to a 90% CI.

Risk analysis is a comprehensive process that involves the identification of threats, susceptibility of IT system's assets and determination of the need of its controls [259]. Therefore, to begin the risk identification stage, we tasked the participants to build on the knowledge of the previous stages of the assessment and determine aspects of the repository service (technology, process) where they had identified a gap and develop a risk scenario around it. We emphasised that unless a threat can exploit the identified vulnerabilities, it is not a risk. For each identified risk, we documented the component involved, supplier, vulnerability, threat actor, impact and existing controls; a taxonomy that complies with ENISA's method of structuring risk information. For each risk scenario, the risk register contained a database of possible vulnerabilities, threats agents and threat types, from which the participants could choose and where new risk factors were mentioned, the database was updated accordingly.

The security effect of the identified risks was made up of the security triad, although the majority were loss of availability risks. Also, having Participant-C involved in the risk identification process meant that we did not have just technical people, experienced in the complexities of systems and processes, but also some with the ability to probe for

new areas of risk [274]. Table 7.16 shows the top ten risks identified in the course of the exercise. The risk register provides sufficient detail that enables the participants and other decision-makers within the organisation, understand the nature of the risk and evaluate it appropriately.

In past case studies, we have shown that by taking a disciplined and structured approach, it is possible to improve the objectivity of cloud risk analysis using our simple Monte Carlo probabilistic method. The use of simulation is well suited to events that are uncertain over time, but it can also be used for different scenarios in which the perception of an event is different from one individual to the other [53]. Here, we use it for the latter. To begin the estimation of risk factors, we reminded the participants of the need to incorporate the effectiveness of the existing controls in protecting against threats, the relevance of the security controls and their extent of implementation. The multidimensional approach of the CSCCRA model also ensures that when estimating the impact of a risk, CSPs can take into consideration factors such as revenues, profits, cost, service levels, regulations and reputation. For the risks in Table 7.16, we got each participant to provide us with an independent estimation of the probability of the risk event (with or without control), frequency and impact cost to a 90% confidence interval. We also clarified the definition of each of the terms to ensure there was no confusion (see Appendix A).

Table 7.17 presents the combined participant estimates for identified risks. At first glance through the participant's estimations, one could say that perhaps some of the participants assumed the identified risks were unlikely to happen, and even when they did, they estimated the impact of such risk was very low. For example, a participant had the upper bound estimation of a risk scenario to be worth £100. As we learnt from case study two, participants always require a reference point to increase their objectivity. So earlier in the assessment, when we discovered that CSP-C is estimated to be worth $30 million, and the repository platform (CSP-C-SaaS) was estimated to be about one-fifth of the company value (i.e. $6 million), we requested that the participants consider this in their estimations. Nevertheless, it is worth noting that some of the identified risks are indirect supply chain risks. Hence it might be challenging to estimate their probability or impact on service disruptions.

Using the CQRA tool, we calculated the risk values for each identified risk. The risk value ranged from £15 to £2,475, which sits between the 65% to 90% percentile of the risk value continuum, after our consideration of the existing controls and confidence in the expert estimations. We rated the participants as having low to moderate confidence in their estimations since they initially found it challenging to articulate the risks of the repository SaaS. Also, there is an assumption among the participants that CSP-C's operational security controls are compliant with best practices, which if investigated is because of their trust in

Table 7.16: List of Security Risks identified by the CSP-C Stakeholders

Risk No	Risk Description	Asset at Risk	Supplier	Vulnerability Name	Threat Agent	Threat Type	Security Effect	Existing Controls
R1.	Compromise of Customer PII data stored in Database	Database, IAM	IaaS-Pr-C-A, CSP-C	Insufficient log auditing, shared platform vulnerabilities, Failure of configuration management, Weak authentication mechanism	Malicious Insider, Privileged Insider	Information/Data leakage, Social engineering, Sabotage, Service outage	Confidentiality, Availability	DB encrypted (provider managed), Separation of duties, Least privilege, Schedule daily backups
R2.	Outage of Repository service due to issue with Database	Database	IaaS-Pr-C-a, CSP-C	Inadequate resource provisioning, Limited redundancy, Lack of monitoring mechanism	Malicious Outsider, Accidental Insider	Malicious probes or scans, DDOS, Fraudulent resource consumption attack, Service outage	Availability	Rate limiting controls on cloud infrastructure
R3.	Degraded performance of the Repository service due to bug in Code (infrastructure-as-a-code)	Source code	IaaS-Pr-C-a, CSP-C, Code-Repo-C	Application/platform vulnerability, Cross-cloud applications creating hidden dependency, Non-optimal change control	Insiders (Accidental/ Privileged)	Non-compliance, Loss of governance	Availability (QoS)	Software release control, rollback, Knowledgeable developers, Code review, Use of framework, Sanitised user input
R4.	Unavailability of data due to hardware failure at storage level	Database, File store	IaaS-Pr-C-a, CSP-C, IaaS-Pr-C-b	Limited hardware redundancy,Lack of supplier redundancy, Lack of monitoring service	Environmental, Political	Supply chain failure	Availability	Application portability, File store control, Scheduled daily backup, Geographic redundancy for DB, Alerting mechanism
R5.	Repository users unable to login due to loss of database integrity	Database (User login), IAM	IaaS-Pr-C-A, CSP-C	Insufficient IAM controls, Weak authentication mechanism	Malicious Outsider, Privileged Insider	Sabotage, Abuse and Nefarious use of cloud service, Service outage	Integrity	Schedule backups, Segregation of duties (non-optimal)
R6.	Exposure of cloud service to malicious attack due to inattentiveness to patch mgmt.	Infrastructure, Code framework	IaaS-Pr-C-A, CSP-C	Application/platform vulnerability, Poor patch management, insiders on provider side	Malicious Outsider, Insiders	Malicious probes or scans, supply chain failure, Sabotage, Loss of governance	Confidentiality, Integrity, Availability	Vulnerability checker on Github, Release/patch management (manual), Locked software versioning
R7.	Degraded functionality of the repository service due to unavailability of reference service	Research Indexer(s)	Indexer-C Reference-C	Lack of supplier redundancy	Environmental	Service outage, Service termination or failure, Supply chain failure	Availability	Error handling in code, Supplier-related controls
R8.	Service outage due to inattentiveness to vendor billing	File store, Database, DNS	IaaS-Pr-C-a, IaaS-Pr-C-b, DNS-Pr-C, CSP-C	Unclear roles and responsibilities, Lack of payment automation, Limited alerting	Insiders (Accidental/ Privileged)	Service outage, Loss of Governance	Availability	Manually checks of email and CSP record with vendor, Onboarding/offboarding with finance team
R9.	Extended Economic Denial of Service (EDOS) on Repository infrastructure	Database, File store	IaaS-Pr-C-a, IaaS-Pr-C-b	Lack of monitoring mechanism, Unavailable or misconfigured security controls, Multi-tenancy	Malicious Outsider	DDoS, Fraudulent resource consumption attack, Loss of governance,	Availability	Alerting on cloud usage,
R10	Outage of Repository Service due to DNS incident	DNS	DNS-Pr-C, CSP-C	Insufficient IAM controls, Limited redundancy, Unavailable or misconfigured security controls, Lack of supplier redundancy	Malicious Outsider, Insiders	Abuse and nefarious use of cloud service, Service outage, Supply chain failure, Sabotage, DDOS	Availability	Supplier-related controls, IAM controls

Table 7.17: CSP-C Risk Analysis result based on CQRA calculation

Risk No	**Probability of occurrence (without control)**			**Probability of occurrence (with control)**			**Impact Cost Estimate (£)**			**Frequency (per year)**	**Risk Value (£) Estimates (without controls)**			**Risk Value (£) Estimates (with controls)**			**Estimated Risk Value (£) based on Existing Controls**
	LB	ML	UB	LB	ML	UB	LB	ML	UB		LB	ML	UB	LB	ML	UB	
R1.	21.4%	59.19%	88.5%	0.00%	1.38%	3.97%	£1,894	£59,231	£305,524	0.15	£0	£125	£271.64	£0	£5,374	£14,011	£1,791
R2.	56.00%	81.18%	97.00%	1.37%	4.93%	11.95%	£130	£638	£2,033	0.10	£0	£3	£15	£0	£51.82	£359	£359
R3.	3.332%	25.48%	63.29%	0.38%	1.92%	4.28%	£34	£637	£1,886	0.49	£0	£5.99	£36	£0	£78	£450.15	£36
R4.	**3.21%**	**16.03%**	**35.87%**	**1.08%**	**2.51%**	**4.00%**	**£144**	**£50,477**	**£303,555**	**0.51**	**£0**	**£647**	**£4,144**	**£0**	**£4,110**	**£22,393**	**£2,475**
R5.	3.77%	25.87%	56.72%	0.49%	1.98%	3.59%	£8	£119	£315	0.09	£0	£0	£2	£0	£3	£15	£15
R6.	4.41%	34.13%	64.31%	0.56%	2.29%	4.68%	£597	£1,735	£3,898	1.56	£0	£63	£321	£0	£949	£5,370	£987
R7.	8.98%	55.95%	97.17%	0.42%	2.52%	7.13%	£2	£63	£216	8.38	£0	£13	£60	£0	£298	£1,558	£486
R8.	1.61%	5.72%	10.69%	0.00%	0.69%	1.47%	£39	£193	£431	1.90	£0	£2.52	£14	£0	£21	£100	£61
R9.	6.89%	27.17%	75.26%	0.51%	2.83%	6.95%	£301	£2,644	£7,715	1.00	£0	£7	£35	£0	£71	£292	£292
R10.	3.65%	24.16%	54.49%	0.54%	2.11%	4.79%	£55	£339	£747	0.37	£0	£3	£16.70	£0	£30	£212	£79

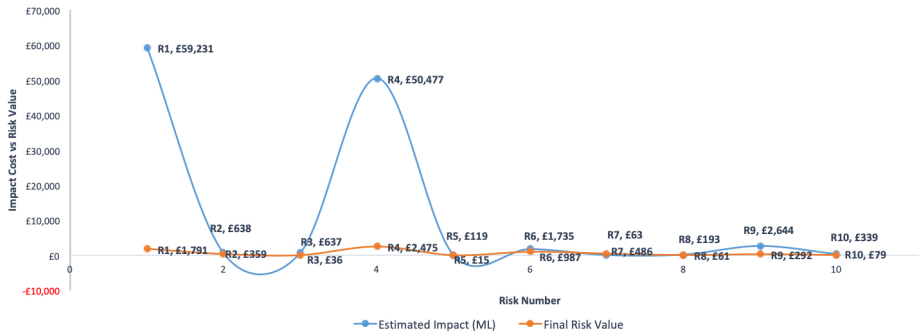


Figure 7.10: CSP-C's Impact Estimate vs. Risk Value Calculation

their IaaS providers and their belief that "no news is good news" [158]. In Figure 7.10, we plot the combined stakeholder estimated impact (ML) with the estimated risk value. The scatter diagram shows the link between the impact cost and estimated risk value, which for many of the risk item follows a predictable pattern, but for others, such as risk **R7** there is an anomaly. This peculiarity is as a result of the increased value of the frequency of occurrence (average of 8.38).

Lastly, considering that our quantitative methods might be new to CSP-C, and seeing that this case study is their first comprehensive risk assessment of the repository platform or any other CSP-C cloud service, we decided to use the opportunity to compare our model with another well-known model. We introduced the participants to the OPTIMIS model, which also targets cloud service provisioning risks and adopts a qualitative method (see section 6.8 for more information on the model). Using the risk scenarios documented in Table 7.16, we got the participants to collaborate and provide us with a qualitative impact and likelihood score. The likelihood and impact values are labelled from 1 to 5 according to their intensity (1-very low, 2- low, 3- medium, 4- high, 5-very high), and the resulting risk level ranged from 1-25. Table 7.18 presents the qualitative value of the identified risks. The risk level ranged from 2 (very low) to 4 (low). We will discuss more on the risk evaluation result of both methods in the next section.

7.3.3 Analysis and Discussion of Assessment results

This case study set out to assess the security risks of the repository SaaS application offered by CSP-C to the academic community. The study was the third and final case study, conducted to validate the applicability of the CSCCRA model. As earlier mentioned, the supply chain element of the model was the main attraction for CSP-C. The provider who was also preparing for their organisation's ISO/IEC 27001 accreditation, were interested in the supply chain security element of the model and identifying gaps in their security processes that could be improved before approaching an external ISO accreditation. Also, seeing that CSP-C did not have an enterprise risk management (structure and set of processes to

Table 7.18: Assessing CSP-C's Risk using the OPTIMIS Model

Risk No	Risk Category	**Risk Description**	**Asset at Risk**	**Vulnerability of Asset**	**Threat to Asset**	**Risk Likelihood 1 (very low) - 5 (very high)**	**Risk Impact 1 (very low) - 5 (very high)**	**Resulting Risk Level (Impact * Likelihood)**
R1.	General	Compromise of Customer PII data stored in Database	Database, IAM	Insufficient log auditing, Shared platform vulnerabilities, failure of configuration management, Weak authentication mechanism	Information/Data leakage, Social engineering, Sabotage, Service outage	4	1	**4**
R2.	Technical	Outage of Repository service due to issue with Database	Database	Inadequate resource provisioning, Limited redundancy, Lack of monitoring mechanism	Malicious probes or scans, DDOS, Fraudulent resource consumption attack, Service outage	2	2	**4**
R3.	General	Degraded performance of the Repository service due to bug in Code (infrastructure-as-a-code)	Source code	Application/platform vulnerability, Cross-cloud applications creating hidden dependency, Non-optimal change control	Non-compliance, Loss of governance	2	1	**2**
R4.	Technical	Unavailability of data due to hardware failure at storage level	Database, File store	Limited hardware redundancy, Lack of supplier redundancy, Lack of monitoring service	Supply chain failure	3	1	**3**
R5.	General	Repository users unable to login due to loss of database integrity	Database (User login), IAM	Insufficient IAM controls, Weak authentication mechanism	Sabotage, Abuse and nefarious use of cloud service, Service outage	2	1	**2**
R6.	General	Exposure of cloud service to malicious attack due to inattentiveness to patch mgmt.	Infrastructure, Code framework	Application/platform vulnerability, Poor patch management, Insiders on provider side	Malicious probes or scans, Supply chain failure, Sabotage, Loss of governance	3	1	**3**
R7.	Technical	Degraded functionality of the repository service due to unavailability of reference service	Research Indexer(s)	Lack of supplier redundancy	Service outage, Service termination or failure, Supply chain failure	1	1	**1**
R8.	General	Service outage due to inattentiveness to vendor billing	File store, Database, DNS	Unclear roles and responsibilities, Lack of payment automation, Limited alerting	Service outage, Loss of Governance	2	1	**2**
R9.	General	Extended Economic Denial of Service (EDOS) on Repository infrastructure	Database, File store	Lack of monitoring mechanism, Unavailable or misconfigured security controls, Multi-tenancy	DDoS, Fraudulent resource consumption attack, Loss of governance,	4	1	**4**
R10	Technical	Outage of Repository Service due to DNS incident	DNS	Insufficient IAM controls, Limited redundancy, Unavailable or misconfigured security controls, Lack of supplier redundancy	Abuse and nefarious use of cloud service, Service outage, Supply chain failure, Sabotage, DDOS	2	1	**2**

systematically manage all risks to the enterprise covering the supply chain and third party risks), the use of the CSCCRA model presented them with a cloud-specific approach for accomplishing this.

Acknowledging that no two case studies can be the same, our approach to assessing the risk of CSP-C-SaaS was quite different. Not only did we have an initial risk assessment questionnaire prepared for the CSP, but we also broke down the risk assessment process, into different chunks, conducting the pre-assessment activities offsite, rather than in-person during the risk workshop. This did not affect the completeness of the assessment. However, suspecting that the vantage point of the supply chain and supplier assessment might have been blurred due to the gap between the different stages, we reminded the participants of the progress made.

As shown in Table 7.16, the risk assessment process covered availability and confidentiality risks including, service failure, insider threat, data loss or compromise, denial of service and other direct and indirect supply chain risks. The value of the top ten risks ranged from **£15** to **£2,475**, an estimation we judged to be low, particularly when compared to the value of the repository platform ($ 6 million). Nevertheless, the qualitative estimation of the same risks using the OPTIMIS model confirmed that the CSP had a low estimation of the identified risks. We posed the question to the participants in our follow-up meeting, where we discussed the result, and the consensus was that they mostly considered the loss of productivity in their impact assessment. According to Participant-C1, "*due to the nature of the repository platform as a piece of hosted software, temporary outages of this product are unlikely to result in paid-back fees, nor are they likely to cause permanent loss to reputation, market share, or data. In most cases, the productivity cost is the only possible or realistic impact cost for us*".

Comparing the CSCCRA and OPTIMIS risk analysis process, as shown in Tables 7.17 & 7.18, we see how the range compression challenge of qualitative methods can introduce errors into the risk assessment process. While knowledgeable cybersecurity experts have argued both sides, the quantitative approach, in this case, has demonstrated the ability to reduce the vagueness in security and assist CSPs with risk quantification and prioritisation. OPTIMIS's use of ordinal scale for simplicity does little to assist decision-makers in reducing the uncertainty that surrounds their cloud risks. This can be illustrated briefly by taking risks R1 & R9, both of which were analysed to be "very low" risks (score of 2) using the OPTIMIS model. Using the CSCCRA, risks R1 & R9 have risk values of £1,791 and £292 respectively. Seeing that the difference in their risk value is almost £1,500, a CSP who is not privileged to have the monetary value of the risks might look to treat both risks alike, without any precise evaluation of options.

Turning now to the identified risks and the analysis process. Loss of Availability (service outage) is often cited as one of the most significant risks of cloud computing. The cloud's reliance on the Internet tops the reasons why it is on the mind of CSPs and customers alike. The participants considered different scenarios in which the SaaS application could suffer an outage, considering the weak security spots in their supply chain and cloud design. This includes Risk **R2**, where the participants identified an availability issue with the database (a critical component) and Risk **R5**, which addressed an outage of the system caused by the loss of data integrity. The CSP had reasonable controls to address each scenario, including having daily backups, assigning user roles and responsibilities and the implementation of an active geo-replication of the database. This, however, do not eliminate the risks, as there are instances where malicious attacks have taken advantage of excessive privileges, tampered with backup media, or even targeted a primary database, forcing a replication of the issue to the secondary instance. Risks **R4**, which happened to have the highest monetary value, referenced the unavailability of the CSP-C-SaaS due to an indirect supply chain hardware failure at the IaaS provider (IaaS-C-Pr-a). With the solution void of supplier redundancy, the recoverability of the application will have to go through a manual process of standing up a new environment, restoring code, backup and customer files, none of which is a minor task. Although CSP-C was adamant that the impact is manageable, we encouraged them to make suitable plans and put measures in place that ensures the business can respond appropriately to such events, and they can recover critical and essential operations to a state of partial or full service, in a short time.

Risk **R1** brought to fore, access control privilege gaps in the way CSP-C managed the repository platform. From our observation, the architecture of the platform did not facilitate efficient user identification, authentication, authorisation and auditability, which made it possible for a malicious outsider or privileged insider to compromise customer PII data. During our discussions, we realised that there was also a situation of human SPOF, where one administrator authorised and managed all privileged user request manually from his email. Due to the size of the development team, this process is functional but insecure. To illustrate the point, the researcher brought up the incident with Code Spaces, a source code-sharing site whose AWS EC2 console got hacked, leading to the deletion of all their data and eventual shutdown of the company [240]. We advised the CSP-C to look into implementing MFA and PAM, where strong password policies can be enforced. To improve on the security controls of their component suppliers, some of the areas we observed CSP-C could benefit from a more stringent access control process includes developer access, operator access, database access and DNS.

The potential for DNS attack was highlighted in Risk **R10**. DNS, which is critical to the operation of a web application has in recent times become an attack vector for attacks

such as footprinting, denial of service, data modification and redirection. We noticed from the supplier assessment that the DNS provider controls were not known to CSP-C. We detected gaps in the access control, logging, and monitoring controls of CSP-C concerning DNS-Pr-C and suggested improvements.

Two risks (**R8** & **R9**), were identified as service hosting risks. For risk R8, the participants identified a situation where the failure to pay a bill, leads to the vendor (DNS, IaaS) shutting down the service. While this is a rare and unlikely situation, hence the risk value (£61.24), it reminded the stakeholders to firm up their payment process, by considering automated means of payment and subscription renewals. Risk **R9** was particularly interesting to the participants, as they had not thought about it before this assessment. Just as the researcher was sharing anecdotes of past incidents in the industry, one of the participants suggested that the risk be added to their risk register. Economic Denial of Service (EDoS) or service provider bankruptcy, occurs where malicious attackers take advantage of the elastic nature of the cloud to scale a service beyond the economic means of the CSP to pay their cloud bills. An incident shared by VivinSandar et al. [319] involved a service targeted by HTTP, XML DDoS attacks from several nodes, which led to the scaling of the service by consuming more Amazon EC2 resources. This risk uncovered some of the inadequacies of CSP-C process around benchmarking their cloud usage. We also suggested that the implementation of WAFs and DDoS scrubber service be considered if the mitigation of this risk becomes a priority.

In summary, while the CSP-C-SaaS has been built to deliver a secure repository service to the academic community, thanks to their highly skilled developers and SDLC process, the most significant risk to the cloud platform will most likely emerge from the insufficient due diligence related to the individual components. CSP-C's approach to security seems to be heavily reliant on "provider default controls", many of which they are yet to update. The SaaS application is not optimised for security, and this is traceable to the organisational culture and the lack of oversight around cybersecurity [83]. From our discussions, it would seem that cybersecurity is not seen as a transit enabler of value to the organisation [118] and as such, it is competing against other priorities for IT spending.

7.3.3.1 Risk Mitigation and Treatment Recommendation

Mitigating cloud risks is most often about implementing additional controls, policies, processes, procedures or by utilising additional technical security features. While not all risks will occur, implementing security best practices ensure that controls will be in place to reduce the impact of those that do. Our assessment showed that CSP-C lacked oversight of some of their critical tasks. Their dependence on a single multi-faceted administrator for their security operations and reliance on vendor controls for their security has potentially

left them exposed to attacks from and through the supply chain. As such, we identify the need for the CSP to implement a risk-based approach with their security. There is an opportunity for the CSP to improve the cybersecurity awareness of their team, implement security policies and procedures, and integrate prevention, response and recovery strategies into their security operations. CSP-C can look into centralising their IAM function, which is currently spread across multiple platforms, and consider implementing multi-factor authentication for all accounts accessing sensitive data or systems.

To identify control measures that would assist CSP-C with their identified risks, we consulted cloud security best practice documentations [98, 267], standard and guidance documents and other online resources. While acknowledging that the implementation of these controls could be costly, may be partially ineffective and have no direct correlation to revenue [32], we maintain that ignoring the known vulnerabilities carries with it more significant consequences. Our risk-ranked recommendations which cover areas such as cloud governance, privileged access management, data protection, change management and redundancy, is presented in the order of their monetary value in Table 7.19. We believe that the suggested best practices will assist CSP-C to improve the agility and robustness of the repository cloud service to a level that is fit for their competitive strategy [328].

7.3.4 CSP-C Evaluation of Model and Case Study Exercise

In keeping with our practice, at the end of the case study, we encouraged the participants to reflect on the model's approach to cloud risk assessment and provide us with some feedback. This gave the three participants that took part in all stages of the assessment an opportunity to evaluate the model. We presented them with a set of evaluation questions on a five-point Likert scale and also furnished them free-text questions, aimed at assessing the strengths, weaknesses, shortcomings, and practicality of the model. Consistent with most case study exercises, the participants identified positive and negative aspects of the assessment process, which we report in this section.

Overall, the feedback from these participants was positive. They validated the applicability of the model to SaaS CSP environments. As shown in Figure 7.11, the participants strongly agreed/agreed with the majority of our statements regarding the advantages of the overall model and its components. They strongly agreed on the usefulness and practicality of the model. There was a consensus on the practical use of the model for assessing cloud risks. Also, there was support for the advantage that the quantitative approach and presentation of risk value in monetary terms bring to decision-making and risk prioritisation. The participants felt the model provided them with valuable insight into their supply chain and informed their decision on ways to improve the security of their cloud service, knowing the different weaknesses of their suppliers. The use of the CSSA tool allowed CSP-C to

Table 7.19: Treating CSP-C's identified risks based on Best Practice and assigning Risk Owners

No	Risk	Risk Description	Existing Controls	Security Best Practice	Estimated Risk Cost	Risk Treatment?	Risk Owner?
1.	R4	Unavailability of data due to hardware failure at storage level	Application portability, File store control, scheduled daily backup, Geographic redundancy for DB, Alerting mechanism	Provider redundancy; Continuous backup (after change); BCP/DR plan; Improved monitoring at storage level.	£2,475.32		
2.	R1	Compromise of Customer PII data stored in Database	DB encrypted (provider managed), Separation of duties, Least privilege, Schedule daily backups	Multi-Factor Authentication; Data Leakage Prevention (DLP); Enforce strong passwords; Cybersecurity training for employees; Have an Incident response plan and implement an incident handling process; Data breach notification process.	£1,791.41		
3.	R6	Exposure of cloud service to malicious attack due to inattentiveness to patch mgmt.	Vulnerability checker on Code Repo, Release/ patch management(manual), Locked software versioning	Automating patch notification and change control process; Automate patch management (e.g. Chef); Develop a patch cycle; Run periodic validation vulnerability scans; Update asset inventory.	£987.00		
4.	R7	Degraded functionality of the repository service due to unavailability of reference service	Error handling in code, Supplier-related controls	Improve supplier redundancy; Supplier selection.	£485.61		
5.	R2	Outage of Repository service due to issue with Database	Rate limiting controls on cloud infrastructure	Implement DR with an alternate provider; Improved monitoring for early detection	£358.79		
6.	R9	Extended Economic Denial of Service (EDOS) on Repository infrastructure	Alerting on cloud usage	Establish resource usage and set limit on cloud spend; Use of DDoS scrubber service; Correctly size the web servers hosting application; Improved monitoring and alerting on anomaly	£292.21		
7.	R10	Outage of Repository Service due to DNS incident	Supplier-related controls, IAM controls	Improve Privileged Access Management (PAM); Central logging of privileged user activity; Segregation of Duties; Dual Control for critical tasks.	£79.24		
8.	R8	Service outage due to inattentiveness to vendor billing	Manually checks of email and CSP record with vendor, Onboarding/offboarding with finance team	Automating Billing process; Set an Auto Top-up level; Establish Roles and Responsibilities and educate staff; Auto-Renew subscriptions.	£61.24		
9.	R3	Degraded performance of the Repository service due to bug in Code (infrastructure-as-a-code)	Software release control, rollback, Knowledgeable developers, Code review, Use of framework, Sanitised user input	Dynamic source code scan; Proactive software patches; Keep Coding simple; Avoid regression and messy code; Employ Software testing resource.	£35.74		
10.	R5	Repository users unable to login due to loss of database integrity	Schedule backups, Segregation of duties (non-optimal)	Improved Logging and Alerting; Database integrity checking; Database encryption; Timestamping; Regular scheduled backup.	£15.37		

conduct a detailed assessment of the security practices of their upstream suppliers. Before now, they had only considered security from an application software perspective, which in itself was not sufficient. According to NIST, one of the principles of cyber supply chain risk management is that organisations need to develop their defences based on the principle that their systems will be breached [199]. NIST goes on to say that cybersecurity is beyond a technology problem; it includes people, processes and knowledge.

Criteria	Strongly Agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Supply Chain Mapping (CSCM)					
The CSCM tool is a good first step in the risk assessment process	♦ ♦	♦			
Identifying and mapping your cloud supply chain enables you to visualise data flow, and assists in thinking about security (CIA) risks.	♦ ♦♦				
Supplier Assessment (CSSA)					
The identified target security factors used in the CSSA tool are appropriate for rating the security of cloud suppliers.	♦♦	♦			
The result of the CSSA improves your understanding of potential cloud risks.	♦ ♦♦				
Quantitative risk analysis (CQRA)					
The process of estimating the risk factors (impact, probability etc.) helps to limit expert subjectivity.	♦	♦	♦		
The risk formula and resulting risk value is a good representation of cloud risk.	♦	♦♦			
The Monte Carlo risk calculation process is easy to understand	♦	♦♦			
Overall CSCCRA model					
Understandability					
The steps of the model are easy to understand	♦♦	♦			
The assessment guidelines and documentation are understandable	♦♦	♦			
Ease of Use					
The model is easy to use	♦♦	♦			
Usefulness and Practicality					
The model is useful for assessing cloud risks.	♦ ♦	♦			
The model's approach to addressing cloud risk is practical for use in the cloud industry.	♦ ♦ ♦				
The result of the risk assessment is reproducible and verifiable.	♦	♦	♦		
The result of the model helps with decision-making and the implementation of mitigation.	♦ ♦♦				

Figure 7.11: CSP-C Participant feedback on the CSCCRA model

When asked how they see themselves applying the model to their environment, one participant reckoned that *"the model's approach will be used in reviewing our current practice and will form part of our ISO/IEC 27001 process"*. The participant feedback also supports our claim that the model supports the periodic evaluation of a cloud service. The CSCCRA model assumes that systems can change over a short period, so CSPs can periodically assess the security posture of their service following the addition or removal of a cloud component.

Also, the case study exercise seems to have stirred the participants to their need of a security culture within the organisation. According to Participant-C1 *"we will consider security when making changes to the cloud environment"*. Another participant mentioned that they hope to use the model to evaluate risk on their other cloud-based products. The participants identified the areas of the strength of the model to include its supply chain inclusivity, its support for different stakeholder opinions and perspectives, its comprehensive approach to risk assessment and its ability to promote valuable discussion amongst stakeholders.

However, on a less positive note, two of the participants commented that some of the quantitative risk concepts were not easy to understand. Another participant was also indecisive about the ability of the model to limit subjectivity, even though he recognised that it was more objective than the OPTIMIS model. While we believe these opinions are based on the exposure of the participants and their lack of understanding of the statistics that underline the quantitative analysis process, we identify a need to simplify the process and make it easy to understand. In simplifying the estimation process for the next phase of the study, which is the development of CSCCRA's web-based application, we plan to reduce the estimated risk factors from four to three, eliminating the probability of risk occurrence without controls. The eliminated factors have been known to cause some confusion with participants. We will also define each of the risk factors in detail, using examples on the help page, to ensure CSPs can use the tool with limited assistance.

Furthermore, there was a consensus that the assessment process was time-consuming, particularly the risk identification phase, although the participants agreed that the process was worthwhile. Some of the suggestions on how to improve the risk identification process included having fewer risks, e.g. having one risk for each significant component/asset, and identifying risks based on already defined questions. While we had no specific basis for having CSPs identify their top ten risks, we thought it was a good number of risk to tracked on the risk register. Also, as regards having a set of questions from which the CSP can identify their risk, we have not found a way to make this generic, seeing that each CSP environment is unique. So far, our approach has been for stakeholders to experiment with different "what-if" scenarios and explore the outcomes of risk under these scenarios. Nevertheless, as we continue to improve the model during and after this research work, we see this process evolving.

Lastly, based on feedback obtained from the end-of-study discussions, it was clear that the participants welcomed the comprehensive level of information the CSCCRA model provided on their supply chain. The participatory nature of the assessment, made them feel included in the identification, evaluation and treatment phases. We are convinced that the transparency effect of the model was realised with CSP-C. Also, the CSCM and CSSA's ability to provide stakeholders with visibility into their supplier security, unfolded gaps

in CSP-C's security controls, causing them to fundamentally question and rethink their established interpretations of CSP-C-SaaS's security posture.

7.3.5 Summary

In summary, the empirical findings from this study provide further support for the hypothesis that the CSCCRA model enables CSPs to understand, manage and make well-informed decisions about their cloud risks. The study validated the applicability of the proposed model to cloud SaaS environments and highlighted the model's ability to capture the context for the cloud application, including aspects of the system that might be overlooked in a traditional asset-based assessment. The individual components of the model, mainly, the CSCM and CSSA tools, uncovered the security gaps in CSP-C's supply chain. The CSCM provided the CSP with a "big picture" of their supply chain and its dependencies, while the CSSA brought to the fore the problem of insufficient due diligence in supplier selection and security control implementation.

With the CSP acknowledging the usefulness of the model and consenting to adopt CSCCRA's processes in the assessment of their other cloud services, we established the practicality of the model to cloud SaaS environments. We observed that the model influenced the participants to think differently about their supply chain risks, estimate risk values objectively, identify ways of improving their security and hold constructive conversations on cloud risks. For CSP-C, we believe the most significant impact of the case study, was the ability of the model to expose the CSP to their lack of oversight around cybersecurity and their need for a security culture within the organisation.

7.4 Case Study Summary

In this chapter, we presented a comprehensive evaluation of the CSCCRA model, using the real-life case studies of three SaaS providers. We investigated two core areas in this evaluation, which are closely tied to research questions RQ3 & RQ4. We chose the case study research method for this phase of the study because it is a comprehensive process that makes use of multiple methods for information gathering, e.g. interviews, observations and questionnaires. Our choice of a multiple case study approach was geared at helping us gather information on the applicability of the model amongst cloud providers with potentially different supply chain arrangement and unique risk management system. The case study was conducted in a systematic manner where we applied the lessons learnt in each case study to the next.

The case study was useful because, through the process, we applied an iterative and continual process of testing our model in real-life scenarios and revising the workings of the model and our presentation of its artefacts. The case studies validated the usefulness and

applicability of the CSCCRA model to CSP environments. Each CSP applied the model to different cloud risk assessment need, and as described in each case, the components of the CSCCRA model provided the CSPs with an insightful view of their supply chain risks. The CSCM simplified the presentation of complex supply chain information using maps, while the CSSA brought transparency to the security posture assessment of cloud suppliers, providing a quantitative measurement of security performance across the chain. The entire risk assessment process fostered collaborative communication among the stakeholders, and the participants acknowledged the ability of the model to bridge existing cloud risk assessment gaps. One highlight of the study was the feedback we received from all the case organisations informing us of their commitment to continue using components of the model in future cloud risk assessments.

In the next chapter, we analyse the combined results of the case studies identifying the similarities and differences between the CSPs and the lessons learnt from the application of the model. Also, we provide answers to two research questions, RQ3 & RQ4, confirming the advantages of CSCCRA's pre-assessment activities and the advantage of the quantitative model over its qualitative counterparts.

Chapter 8

Combined Case Study Discussion and Findings

In this chapter, we discuss the result of the three case studies and extract the important findings from the use of the model in these CSP environments. Also, in this chapter, we provide answers to research questions **(RQ3)** & **(RQ4)**. RQ3 seeks to investigate whether the application of the cloud pre-assessment tools, i.e. CSCM and CSSA, complemented the risk assessment process and improved CSPs understanding of their cloud risks. Likewise, RQ4 evaluates the advantages of a quantitative risk assessment model over its qualitative counterparts in quantifying loss exposure, reducing uncertainty and promoting better decision-making.

8.1 Case Study Discussion

To avoid repeating the information already contained in the individual case studies, we conduct a cross-case analysis of the risk assessment process. This analysis describes how each case organisation with unique risks, security controls, budget, countermeasures and risk assessment process, applied the CSCCRA model to their environment. We extract the contextually specific details of each case organisation and discuss how our approach supports decision-makers in understanding their cloud/supplier security posture and evaluate their cloud risks. In Table 8.1, we compare the case organisations, after which we attempt to offer a common explanation to the challenge CSPs face in assessing the risks of their cloud service and how the CSCCRA model complements the cloud industry's best practice. The high-level cross-case analysis presented in Table 8.1 highlights the size of the organisation, their motivation for participation, the goal of the assessment, range of the estimated risk values, and evaluates the maturity of each CSP's security operation and their cybersecurity posture. We broke down the last two themes into sub-themes, and we describe each of the sub-themes below:

- **Awareness of Supplier Security processes**: Here, we gauge the CSP's knowledge of their supplier security processes and how they leveraged it to improve their cloud security operation.
- **Approach to Supply Chain Risks**: This sub-theme looks into the CSP's attitude to supply chain risk and evaluates if CSP awareness promotes robust processes and implementation of security controls.
- **System Availability**: This sub-theme looks into the approaches taken by the CSP to ensure the high availability of the SaaS application.
- **System Security**: Here, we assess the operational procedures followed to keep the SaaS safe from remote attackers and other cyber threats.

The empirical findings of these case studies provide convincing evidence of a strong association between the lack of awareness/visibility of supplier controls and the subjectivity synonymous with cloud risk assessment [309]. While the supply chain mapping activity provided cloud providers with a big picture of their dependencies, the process of assessing the supplier security posture in each of the case studies, took longer than expected. Because the CSPs had insufficient information on their suppliers' technical and operational security processes, they spent considerable time trying to find information that can support their rating of the security target dimensions. The case studies showed that cloud stakeholders continue to prioritise cost, service suitability, vendor reputation and functionality, over security [20]. None of the three SaaS CSPs was fully aware of their supply chain, their supplier processes or the security posture of their suppliers.

The Cloud Security Alliance (CSA) was right in naming insufficient due diligence among the top threats of cloud computing [67]. Particularly with CSP-A and CSP-C, their knowledge of their supplier security processes was superficial, and as a result, they did not leverage the extended range of security controls available to them by their suppliers. Also, in comparison to the others, CSP-C did not have an excellent grasp of the security of their cloud service and the assurance of their security was subjective. They operated their cloud environment on the assumption that hosting the service with a reputable IaaS provider, having operational systems and performing within acceptable limits, meant that the majority of their security risks were mitigated. This phenomenon of creating a list of supposed essentials that can help CSPs achieve compliance without being contextual or risk-focused is often referred to as 'tick box security' [137].

Across the SaaS organisations, security control gaps could be noticed in areas such as central logging, proactive monitoring, privileged access management, multi-factor authentication, supplier and data redundancy, encryption and key management, and database

Table 8.1: Cross-Case Analysis of the Three SaaS Organisations

No	Theme	Sub-Theme	CSP_A	CSP_B	CSP_C
1.	Size of the Organisation		51 - 250 employees	10 - 50 employees	10 - 50 employees
2.	Motivation to Participate		The invitation to participate coincided with a request for the CSP to conduct a risk assessment of the SaaS application by their funding body. CSP was also interested in the supply chain aspect of the model.	The CSP had just conducted an unsatisfactory assessment of their cloud service using the traditional ISO/IEC 27001 methodology. Also, our supply chain inclusive approach appealed to the CSP.	Case study presented an opportunity to, for the first time, assess the risk of a cloud service. CSP was also interested in knowing more about their supply chain security and having their risks presented in monetary terms.
3.	Goal of Assessment		To understand the security and privacy risks of the social platform and implement controls to mitigate them.	To assure the quality and integrity of the asset management SaaS solution, while assessing its security gaps.	To identify the security gaps in the repository platform and gaps in the organisation's security practice as they prepared for their ISO 27001 accreditation.
4.	Estimated Risk Value		£325 - £26,513	£90 - £36,357	£36 - £2,475
5.	Maturity of Security Operation				
a.		Awareness of Supplier Security processes	CSP-A had a past working relationship with their main supplier before implementing the social care platform and were abreast with their security offerings. However, they relied more on functionality and cost in selecting other suppliers, and had no tangible knowledge of their security processes.	CSP-B, perhaps due to the nature of their business, carried out security due diligence on their suppliers processes. The architecture of their platform also shows they implemented complementary security solutions to address supply chain gaps and improve their security posture.	CSP-C relied on vendor reputation and suitability of supplier platform in choosing their main supplier.They were more interested in the day-to-day operations of the repository service and paid less attention to the security offerings of their critical suppliers, which could have improved the posture of their service.
b.		Approach to Supply Chain Risks	Some of CSP-A processes showed that they considered supply chain risks, but the CSP lacked fundamental processes to deal with supply chain failure e.g. DR. Being a ISO-27001 compliant company, they were used to looking for risk within their own processes and did not extend this approach to their vendors.	Although CSP-B was not aware of all their dependencies (particularly on their main supplier), the security architecture of the asset tracking platform put in compensating controls to address supply chain risks. The CSP prioritised security and had robust processes to manage most of their known supply chain risks. However, the model exposed the CSP to some unique supply chain risk scenarios.	Before the case study, it seems that CSP-C had not really considered their supply chain as a source of risk to their platform. While the CSP had recovery solutions for their critical data, their security architecture did not include controls to mitigate supply chain risks.
6.	SaaS CSP Security Posture				
a.		System Availability	CSP-A hosted their cloud application with one of the "Big Four" cloud providers, and took advantage of the CP's redundant infrastructure. However, the SaaS application is not built to be fault tolerant and an outage within the cloud provider environment or in one of the critical suppliers such as DNS, means an outage of the SaaS service.	Through the supply chain mapping, we realised that CSP-B is heavily reliant on their infrastructure provider (a member of the Big Four), and many of their other suppliers also hosted their services with this provider. On face value, the system availability of the asset tracking platform and the compensating controls implemented are sufficient. However, the CSP can benefit from maintaining a minimal operation with an alternate supplier.	CSP-C application is also hosted on a "Big Four" platform and as such inherits the redundancy built into the cloud provider's infrastructure. The CSP also implemented a minimal data backup solution with another Big-four provider to ensure they can recover from a failure. However, the CSP have not considered the critical supplier dependencies in the overall availability plan and as such, do not have a highly available platform.
b.		System Security	In the course of the assessment, we realised CSP-A prioritised confidentiality risks over availability and integrity risks. In addition to the secure hosting of the SaaS, the CSP put in compensating controls such as logging and monitoring to enable them react to attacks on their platform. Nevertheless, the CSP can improve on its operational procedures by implementing MFA, database encryption, web application firewalls and having a DR and incident response plan.	CSP-B have controls in place to identify, detect, respond and react to cyber threats. The controls they lack are preventive controls. This control includes implementing solutions like intrusion prevention systems (IPS) and WAFs. While they operate a small security function, the CSP can do more with separating user roles and logging privileged access.	CSP-C have a good software development lifecycle process, which helps with keeping bugs and vulnerable patches out of the cloud application. However, the CSP lacks technical security controls particularly around central logging, monitoring and privileged access management. The CSP need to look into implementing security controls beyond the default vendor settings. Nevertheless, the biggest risk of CSP-C is related to their lack of supplier due diligence and poor security culture.

integrity checking. We emphasised to CSP-A and CSP-C during the case studies that implementing PAM using MFA should be seen as a minimum requirement for managing SaaS applications. Also, perhaps due to the sizes of the business and their relatively small workforce, we noticed that the same individuals performed multiple roles, and in many cases, constituted a single point of failure. For instance, in CSP-B, the CEO doubled as the CTO and Chief Architect. Likewise in CSP-C, the CTO was responsible for the technical operation (authentication, backup, security, indexing, availability, and DNS) of the cloud service and acted as a SPOF to the organisation. The CSCCRA's approach to cloud risk assessment enables weak spots such as those listed above to be identified as the stakeholders decompose the cloud service to improve their understanding of its underlying elements. As ENISA rightly points out, the identification, analysis and evaluation of threats and vulnerabilities is the only approach to understanding and measuring the impact of the risk involved, which also helps to determine the appropriate measures and controls to manage them [97].

Comparing the estimated risk values across the case organisations, we see that similar risks are estimated differently. For example, CSP-A's risk of DDoS (R2) was evaluated to cost them £5,383, while a similar risk experienced by CSP-B (R6) is only valued at £778, a difference of £4,607. This variation in risk cost can be due to many reasons, some of which are: the subjectivity of participants, stakeholders unfamiliarity with the impact of a risk, or value of cloud service. On the evaluation of risk factors, we found out from our sensitivity analysis of the model, that risk value output was most sensitive to the frequency of risk occurrence input variable. The model's sensitivity to the frequency input variable was also seen in the evaluation of at least three risks during the case studies, where the final risk value was higher than the most likely impact cost. So, depending on how high or low the frequency risk factor is estimated, there can be a considerable gap in the estimated risk value.

Therefore, acknowledging the imperfections of the risk estimation process and by extension, the estimated risk value, we caution against CSPs using the model solely to present risk values in monetary terms. While this remains an advantage of the model, we are aware of the corruptibility of the process, where the estimation of risk factors can become a game among the participants, notably when a reward is promised to the participant with the highest or lowest estimate [86, 122]. Besides, in situations where a CSP is conducting the risk assessment to make a case to the board of directors on the need to invest in security controls, there is a possibility that extreme estimations can be made. While we did not notice such game playing in the case organisations, we cannot rule it out. That said, we encourage CSPs to identify the meaningful signals in the assessment result and prioritise their risks accordingly. Likewise, we believe that the value of the model, as attested to

by the participants lie in its ability to provide CSPs with an understanding of their risks, an opportunity to objectively evaluate their security controls, verify supplier processes and identify weak spots in the supply chain. As seen in all the assessment, the participatory nature of the model, also encouraged discussion among stakeholder and presented the participants with a level playing field to discuss the security of the cloud system from their vantage point.

The inclusivity of the CSCCRA model revealed how stakeholder participation and the view of the bigger picture of the supply chain could reveal rare and often overlooked security risks. For example, while assessing CSP-A risks, the divergent thinking by stakeholders led to the discovery of an often overlooked phenomenon in IT risk assessment, i.e. a situation where the ToA (cloud service) is also a threat agent (e.g. spreading malware) [258]. CSCCRA is a comprehensive cloud risk assessment model, which accounts for the role IT infrastructure and third parties play in a risk scenario. The model adds value to the cloud risk assessment process by providing transparency into the underlying factors involved in the identification and analysis of the risks. The decomposition of risk into its various risk variables showed some promising signs of taking away part of the subjectivity of the risk estimates. While our method does not rule out the "Black Swan Effect" [302] i.e. extreme and unpredictable events with enormous consequences, it improves the expert subjectivity in risk estimations, particularly in situations where no historical data exists. We argue that due to dynamic and rapid changes in cloud technology and the complexity of its supply chain, it is impossible to rule out the unknown unknowns (Black Swans). As such, organisations need to adhere to a comprehensive risk model (e.g. CSCCRA) and support their security governance, which helps with managing most of the possible risk scenarios and some rare ones.

To answer **RQ3**, both CSCM and CSSA tools, complemented the risk assessment process and improved CSPs understanding of their cloud risks. Knowing that insufficient due diligence increases cybersecurity risk [208], the CSCCRA model improves the visibility of security control across the supply chain. Our approach produced a more tangible result in the area of operational and infrastructural security risks, which would have been hidden from the CSP if they only assessed their risks using expert intuition or other traditional methods, which lacked the supply chain-inclusivity of the CSCCRA model. The supply chain map helped with the provenance (traceability) of a cloud service, maintaining an end-to-end record of the entities involved in the delivery of the service and their underlying dependencies. Likewise, the supplier security assessment brought transparency to the security risk rating of cloud suppliers, providing a quantitative measurement of security performance across the chain, identifying the inherent risks and comparing suppliers based on their cybersecurity posture. The resultant effect of the pre-assessment activity is that

it improves the objectivity in stakeholder estimation of risk factor values using the CQRA, which invariably increases the justifiability of cloud risk assessment results.

Also, to answer **RQ4**, the result of the case study showed that the structured, systematic and inclusive approach of our quantitative model within SaaS organisations yielded objective and defensible risk assessment results. The CSCCRA improves human judgement on security risks, applying techniques such as calibration, subjectivity probability, collaboration and decomposition of factors [143]. Acknowledging that presenting risk values (based on numerical operations) to decision-makers without a context will be too abstract [129], the CSCCRA model improves the risk presentation process by providing transparency into the underlying factors involved in the identification and analysis of the risks. The empirical findings from the case studies show that our proposed model addresses the efficiency and statistical robustness challenge synonymous with quantitative models [261]. When compared to existing qualitative approach as shown in case study three (using the OPTIMIS model), the quantification process of the CSCCRA and its presentation of risk value in monetary terms was found to promote cost-effective risk mitigation and optimal risk prioritisation. Participants across the case studies were impressed with the model's ability to capture the context for the cloud application, including aspects of the system that might be overlooked in a traditional asset-based assessment. The decision of the CSPs to continue to adopt the model's approach in assessing their other cloud services also confirms the advantages of our quantitative approach over its qualitative counterparts.

While it could be argued that the positive results of the case study validation were because the CSPs who took part in the exercise had gaps in their security, which the model was able to identify and suggest improvements, we caution against the rebuttal of the case study results. It is imperative to bear in mind that we did not influence the choice of the CSPs. However, it is possible that the CSPs chose to participate in the case study because they realised the inadequacy of their security controls and wanted an assessor to help them identify their risks. As we continue to trial the model, even after the DPhil process, we envisage that an ideal organisation for a fourth case study will be a CSP who is compliant with industry standards, has a good security culture, maintains an information security function, and has a good grasp of their supply chain. In such an organisation, it will be challenging to predict the usefulness or applicability of the model, but we can hypothesise that if the organisation does not have a supply chain map of their service or conduct a regular supplier assessment, the model will still be valuable.

As we have seen throughout the case studies, the supply chain remains a blind spot for many CSPs, and the inadequacy of CSP's security controls are revealed when considered in relation to the vulnerabilities of the supply chain. For example, the recent report by the NCSC uncovered 70 full copies of 4 different OpenSSL versions, ranging from 0.9.8

to 1.0.2k used in Huawei products, many of which had publicly disclosed vulnerabilities and are unsupported [55]. Considering the firm's size and the possible maturity of their security function, this should have been noticed and dealt with. However, seeing that it was not discovered, we believe such circumstance can benefit from the decomposition process included the pre-assessment stage of the CSCCRA model.

Lastly, bearing in mind that the successful application of the CSCCRA model to the three case studies cannot be easily generalised to all cloud delivery and deployment models, we make a case for the generalisation of the theoretical propositions that the model represents. We see from the results of the assessments and participants feedback, how the systematic use of this supply chain-inclusive model presents stakeholders with a bigger picture of their cloud risk landscape and increase their objectivity during risk estimations. However, we recognise the need to improve stakeholder's estimation of their asset and impact cost during the risk analysis phase, as some participant estimations continue to show signs of extreme subjectivity. This subjectivity was exacerbated by our inability to conduct a vulnerability assessment of the SaaS application in real-time, as a complement to the risk identification phase. Although none of the CSPs had a recent vulnerability report before the case study, they were also reluctant to conduct one. This meant that we employed best-efforts in confirming the susceptibility of the cloud assets to the potential vulnerabilities and in estimating risk factors.

In summary, the empirical results derived from the case organisations confirmed the applicability and validity of the conceptual model presented in Chapter 6. The strengths of the model's approach as identified by the participants include its supply chain inclusivity, its support for different stakeholder opinions and perspectives, its comprehensive approach to risk assessment and its ability to promote valuable discussion amongst stakeholders. The case study results confirm the ability of the model to meet a wide range of cloud provider risk assessment needs. Through these case studies, we observed how participatory research [41] caused science and practice to meet, interact, and develop an understanding of provisioning risks and security in the cloud. The case organisations recognised CSCCRA as an objective risk assessment model and acknowledged that the lack of statistically reliable and relevant past data on cloud risks is no longer a deterrent to quantitive risk assessment [112, 143].

8.2 Case Study Findings and Conclusion

These case study results, concludes our three-staged approach to validating the usefulness of our proposed model in assessing cloud provider risks. The first stage was an *Author Evaluation*, where we determined if the model's processes met our initial criteria. The second was *Domain Expert Evaluation*, where we got domain experts (industry and academia) who

were not involved in the process of developing the model, to assess the model for its applicability, practicality and usefulness. The *Case Study Evaluation* was the third and most demanding of the three stages, but it was also the most rewarding. We initially struggled to get SaaS companies interested in taking part in the exercise, due to organisational resource constraints, and legal and confidentiality concerns. Nevertheless, the rigorous process followed to validate the model with the participating CSPs yielded insightful information which helps us to improve the overall risk assessment process and develop a practical web application.

Seeing that it is a good audit practice to start with something small, and to audit from the outside in [269], the CSCCRA's approach to cloud risk assessment identifies the individual components that comprise the cloud service and attempts to assess the suppliers of those services. By mapping out the supply chain using the CSCM and rating the suppliers on their implementation of security factors, the model can identify the weakest link, which represents the most likely source of cyber exposure. These security factors include the activities, techniques, technologies, policies and procedures that enable the CSP to achieve a secure cloud service. The CSSA tool is not just meant to improve expert accuracy with identifying weak links; it also improves the transparency, consistency, adaptability and speed of these decisions. The resultant effect of the pre-assessment activity is that it improves the objectivity in stakeholder estimation of risk factor values using the CQRA, which invariably increases the justifiability of the risk results.

The main conclusions drawn from our case studies are summarised as follows:

- **Finding 1:** Empirical evidence extracted from the case organisations suggests that assessing cloud risks remains a challenge to cloud providers. Two of the three case organisations who although were concerned about their cloud security risks did not have a structured process in place to assess those risks. We discovered that the application of the traditional assessment frameworks within the three case organisations was to confirm their adherence to security standards (processes) and did not necessarily assure their security. There are only four technical domains within the ISO/IEC 27001 framework, and these domains are not sufficient in themselves for conducting the technical security assessment of a cloud service [28, 153]. As such, these traditional frameworks, which are mainly targeted at supporting organisation-wide assessments, cannot be manually fitted to assess the overall risks of SaaS providers.

- **Finding 2:** The empirical evidence supports our hypothesis that the application of the CSCCRA model to cloud environments, addresses the cloud's insufficient due diligence challenge [208], by increasing visibility into the security controls of cloud suppliers. A recurring theme through the case studies was the ability of the model

to provide stakeholders with the "big picture" when addressing cloud risks. Statistics have shown that many of the most severe breaches have happened to suppliers of major companies and not directly on the company's infrastructure, yet the impact is the same [314]. According to a Forrester survey [132], third parties were responsible for 21% of the confirmed breaches in 2018, an increase from the 2017 data. From the case studies, we learnt that the structural analysis of the interdependence between the various components of the cloud service reduces the CSP's blind spots. The empirical findings also show that the application of the model causes stakeholders to rethink their established interpretations of the cloud service's security, question their initial supplier selection and re-visit their design strategies.

- **Finding 3:** The study confirmed that the application of mathematical operations to cloud risk assessment, promotes transparency. The CSCCRA model required stakeholders to document all their assumptions about the cloud service, its suppliers and their security posture. According to the participants, this approach was useful in increasing the objectivity and justifiability of the risk estimations. The structured format of the assessment also ensures that the process is repeatable and understandable to a wide range of stakeholders. All three case organisations confirmed that the presentation of the risk value in monetary terms gave them a more accurate view of their cloud risk and provided a basis for comparing mitigation cost and future risk assessment results.

- **Finding 4:** The findings from the case organisations substantiates the advantage of a combined stakeholder approach to risk estimations over the siloed method. The risk analysis phase allowed multiple business and technical stakeholders to take part in the identification, estimation and evaluation process, to combine expert knowledge about the cloud service. This approach yielded positive results, particularly with the risk estimation, where experts' subjective confidence (overconfident or underconfident) was checked, to allow the risk assessor to provide a reasonable single risk value to decision-makers. The process allows stakeholders to discuss the security of the cloud service, which they had no prior opportunity to do, due to their busy schedules or organisation structure.

- **Finding 5:** The study findings enforce the need for CSPs to re-visit their cloud strategy during the risk assessment process. Applying the CSCCRA model, CSPs can evaluate if their current cloud setup is still fit for purpose while reviewing the suitability and effectiveness of existing security controls. As seen with CSP-B, using the model caused them to make new design decisions to align the cloud service with the expectation of their customers and improve their service delivery. Organisations

should see the dynamism of the cloud as a call to continuous security and design improvement, and the CSCCRA has exhibited signs of being a model that can assist CSPs in their cloud transformation journey.

- **Finding 6:** The empirical findings support the CSCCRA's proposal for assisting CSPs to conduct a continuous assessment of their security risks. With the use of the CSCM and CSSA tools, CSPs can identify suppliers who no longer meet their security, legal or jurisdictional requirements, while considering alternatives. Seeing that the dynamic, distributed and multi-tenant nature of the cloud exposes it to various risks and uncertainties, the application of our model, despite its static nature, confirmed that a systematic and proactive approach to CSP SaaS risks helps with the continuous assessment and management of resulting risks. In cases where a gap is detected in a supplier control, CSPs can proactively implement a safeguard to protect their service from potential threats.

- **Finding 7:** The findings from the case organisations validates the applicability of the model to different SaaS CSP needs. The case studies showed support for the usefulness of the model is assessing risks involved in the design, deployment, configuration, or operation of the cloud. As a result of the assessment, we observed each CSP re-visiting an aspect of their initial design while looking to tighten up their security controls. This approach is also known to boosts customers' trust. According to Khan et al. [170], any solution that provides the CSP with continuous visibility of its overall risk landscape contributes to the viability of the service.

In summary, while it seems like much progress has been made in cloud risk assessment particularly from an academic standpoint, our case studies have shown that the practical aspects of assessing cloud provider risks are still relatively unexplored. We found out that CSPs are still in the dark as to how best to identify, estimate and mitigate their supply chain cloud risks. These practitioners struggle with security risk assessments. They find the process of understanding their risks, measuring their security and calculating their return on investment burdensome. No wonder many organisations have largely discounted risk assessment results, with some not bothering to conduct a systematic analysis of their service and others outsourcing the process to external consultants.

8.3 Towards a Capability Maturity Model for Cloud Risk Assessment

In this section, we characterise the different stages of organisational maturity in cloud risk assessment. According to Christopher [316], a maturity model is a set of characteristics,

attributes, indicators, or patterns that represent capability and progression in a particular discipline. A maturity model helps to understand the capability of an organisation and assess the maturity of their processes.

While this was not initially part of our research plan, the findings emerged organically through the rich data gathered from the three case study exercises and our conversation with other cloud based organisations. We measure the progress of each organisation using maturity indicator levels ranging from stage 1 (chaotic/ad-hoc) through to stage 5 (proactive/strategic). The five stages presented in Table 8.2 leverages the knowledge in common capability maturity models [49, 133, 316] and the criteria that make up each of maturity level is a pointer to each organisation's attitude to risk management, and the processes they have in place to address cloud risks.

With the increased awareness of cloud cyber threats emanating from the supply chain, there is a need to objectively assess and reliably measure the risk assessment maturity of providers and suppliers involved in the delivery of cloud services. Using the metrics identified for each stage of the CMM in Table 8.2, we rated the three case organisations. Both CSP-A and CSP-B were rated as belonging to Level 2 (repeatable) of the CMM, while CSP-C was evaluated to be in Level 1 (ad-hoc). While both CSP-B and CSP-C do not have an ISO/IEC 27001 accreditation, the distinction between them lies in their awareness of cloud risks and the strategy involved in cloud risk management. CSP-C is heavily reliant on individuals for success (e.g. CTO). Its management's lack of oversight of cloud service risks and their inconsistent risk decision-making contributed to their Level 1 rating. To enhance its rating, CSP-C's management will need to improve the security culture within the organisation. We believe this will happen naturally as they go through the ISO/IEC 27001 accreditation, and apply the lessons learned to their cloud risks.

CSP-B, despite the size of their security function, met most of the criteria of Level-2. Compared to the other two, they had a defined strategy for cloud selection and a sound awareness of the supplier's security processes. As for CSP-A, one can say that their compliance with an international standard (ISO/IEC 27001), contributed to the success of their cloud risk assessment process. Nonetheless, they are still some way from attaining Level 3 on the CMM scale, even though their attitude to cloud risk management shows promising signs of improvement. An example of their attitude to risk is that following our case study exercise, they called the researcher to discuss the risk treatment suggestions in more detail to determine which controls to prioritise. This attitude highlights the merits of the CSCCRA model.

Our case study using the CSCCRA model exposed SaaS organisations to areas where their controls and processes were inadequate and provided them with suggestions on how to

Table 8.2: Capability Maturity Model for Cloud Risk Assessment

Level 1 (Chaotic/ Ad-hoc)	**Level 2 (Repeatable/Intuitive)**	**Level 3 (Defined/Emerging)**	**Level 4 (Measurable/Matured)**	**Level 5 (Proactive/Strategic)**
1. No documented cloud risk assessment process. 2. Provider/Supplier selection based on reputation and cost. 3. No management oversight. 4. Success depends on key individuals. 5. Expert advice rules. 6. Risk decisions are inconsistent.	1. Awareness of cloud computing risks. 2. Defined strategy for cloud selection. 3. Cloud risk management process initiated. 4. Cloud specific roles assigned to key individuals. 5. Cloud risk severity scale defined but qualitative. 6. Risk decisions are based organisational policies.	1. Risk management framework addresses cloud risks. 2. Established metrics for CSP selection. 3. Defined security controls for addressing cloud risks. 4. Management oversight of cloud risks. 5. Cloud supplier dependencies based on established criteria. 6. Risk assessment is part of the procurement process. 7. Risk severity scale includes quantitative ranges. 8. Risk decisions are based on defensible and up-to-date information.	1. Established cloud decision making process. 2. Rigorous risk assessment methodology (Quantitative). 3. Continuous monitoring of cloud risks and RA process. 4. Risk assessment framework includes the wider cyber supply chain. 5. Strategic cloud risk prioritisation with management review. 6. Up-to-date risk register, with an aggregate view of organisation's cloud risk and risk appetite.	1. Automated cloud risk assessment process. 2. Proactive cloud decision making. 3. Predictive risk analytics including supply chain. 4. End-to-end supply chain risk governance and supplier optimisation. 5. Maintain the visibility of the risk landscape to support well-informed cloud decisions. 6. Feedback loop for continuous development of cloud risk assessment process.

improve. Therefore, we believe that the use of the CSCCRA model for the continuous assessment of cloud risks will result in cloud provider organisations progressing along the scale of maturity indicators, moving from Level 1 (chaotic/ad-hoc) to Level 5 (proactive/strategic).

In conclusion, we hope that this risk assessment CMM will be widely accepted within the cloud community. We believe that its use will improve stakeholder confidence in cloud suppliers. The CMM will make it possible for cloud organisations to know the level of their partner's maturity, monitor their improvements, and benchmark their performance against other alternative suppliers. Also, seeing that all cloud providers will be striving to attain the proactive level of maturity (level 5), this will eventually reduce cyber risks in the supply chain and improve the risk management strategies of cloud stakeholders.

Chapter 9

System Development - Implementing CSCCRA as a Web Application

In this chapter, we build on the result of the model's validation with CSPs (chapters 7 & 8) to develop our initial prototype into a web-based risk assessment application. Seeing that the prototype used for the case studies was an integration of excel spreadsheet macros and commercial off-the-shelf (COTS) applications, we proceeded to replicate the functionality integrated into the prototype and improve the usability of the tool. Moreover, the nature of the initial prototype meant that it could not be migrated to the cloud, where it can be assessed by CSPs who need it. Furthermore, as we mentioned in the literature review, only a small amount of proposed models have been developed into usable tools for cloud risk assessment [113]. Therefore, to address this gap and promote the use of the CSCCRA model within the cloud industry, we designed, developed and evaluated the CSCCRA web application. In the following sections, we describe how we implemented our design of the web application and evaluated it with researchers and professionals in the cloud industry.

9.1 System Development

As with all good developments, our design took advantage of some user-centred design principles including active user involvement, simple design representation, prototyping and the use of usability champion [126]. To meet the requirements we set for the application in section 4.4, and comply with the design of the web application in Figure 4.6, we decided to build the tool using the Python programming language. Python is a fast, powerful and open-source programming language that integrates systems effectively [231]. We implemented the application using Python because of its vast array of predefined functions that helps to simplify Monte Carlo Simulations, and the easy integration of Python with the Hypertext Markup Language (HTML) using web frameworks such as Flask and Django. In deciding

between the two main Python frameworks, i.e. Flask and Django, we chose Flask because it is easy to setup, flexible and is considered to be more explicit than Django [195].

To encapsulate all of the web application's attributes and behaviour, we developed a model. We expressed the relationship between the objects and describe the web application using a Unified Modeling Language (UML) class diagram (see Figure 9.1). According to Sommerville [292], class diagrams are used when developing an object-oriented system model to show the classes in a system and the associations between them. As shown in Figure 9.1, the structure of the designed software was conceived to mirror the risk assessment steps of the CSCCRA model. Each class in the UML diagram represents an essential part of the CSCCRA assessment process. Except for the registration and user login page, the risk summary page and the help page, all other web pages included in the web application represents a part of the initial prototype and a stage in the CSCCRA model. We scoped our implementation to aspects of the model that demonstrates our core research idea and gives insight into how CSPs will use the model to assess their cloud risks.

In implementing our design, we installed Python 3.5.2, which had SQLite3 included in the standard library [231]. SQLite provides a lightweight disk-based database, without requiring a separate server process, which was sufficient for this stage of our development. To apply cascading style sheets (CSS) to our HTML webpages and to save time building the web application, we downloaded a free, fully responsive HTML5 site template [8], which was released under the Creative Commons Attribution (CCA) 3.0 license[3]. Using the Flask framework v.1.0.2, we placed all HTML files into folders called templates while the CSS, javaScript and images, were stored under the static folder. Using our Python code, Flask takes care of the server-side processing, receiving HTTP request through the webpages and dealing with those requests. All user inputs, including the identification of SaaS components, supplier identification, risk identification, risk analysis, and the evaluation of cloud risks were implemented through the Python code. Figure 9.2 is a screenshot of the application's homepage after login, while Figure 9.3 shows the process of running the web application from the command-line interface (CLI). As shown in Figure 9.3, the app object (app.py) is an instance of the Flask object, which acts as the central configuration object for the entire web application.

The web application was designed to provide a good user experience (UX). Consciously, we did our best to ensure that the navigation was intuitive, input methods were consistent, and there was a visual hierarchy to the data. As earlier mentioned, the three case studies conducted to validate the usefulness of the model, provided a background for our approach to this tool. While we recognise this might not pass as doing proper user research on the

[3]Miniport is a free, fully responsive HTML5 site template designed by AJ for HTML5 UP & released under the CCA license.

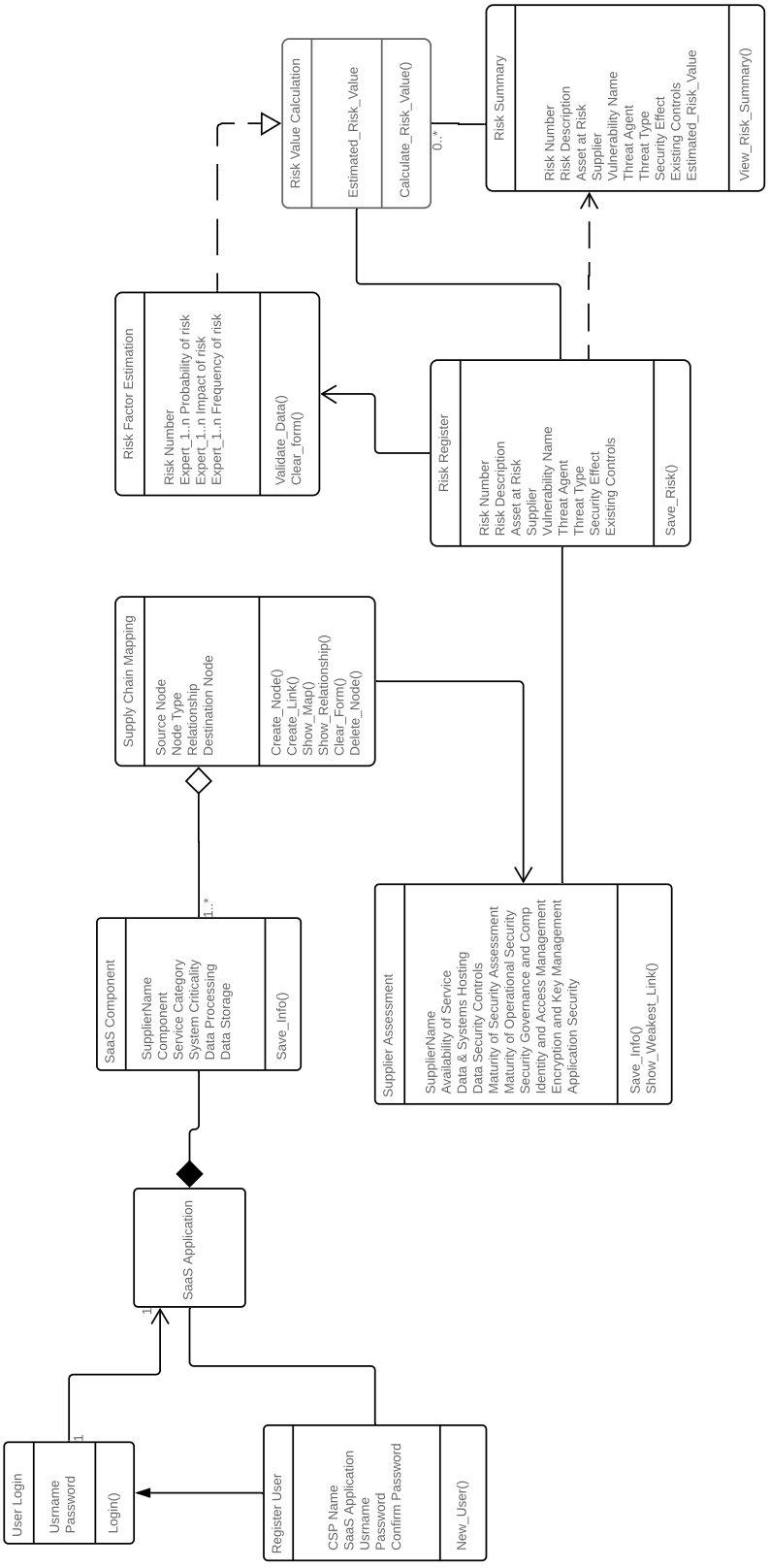


Figure 9.1: UML Class Diagram of the CSCCRA web application

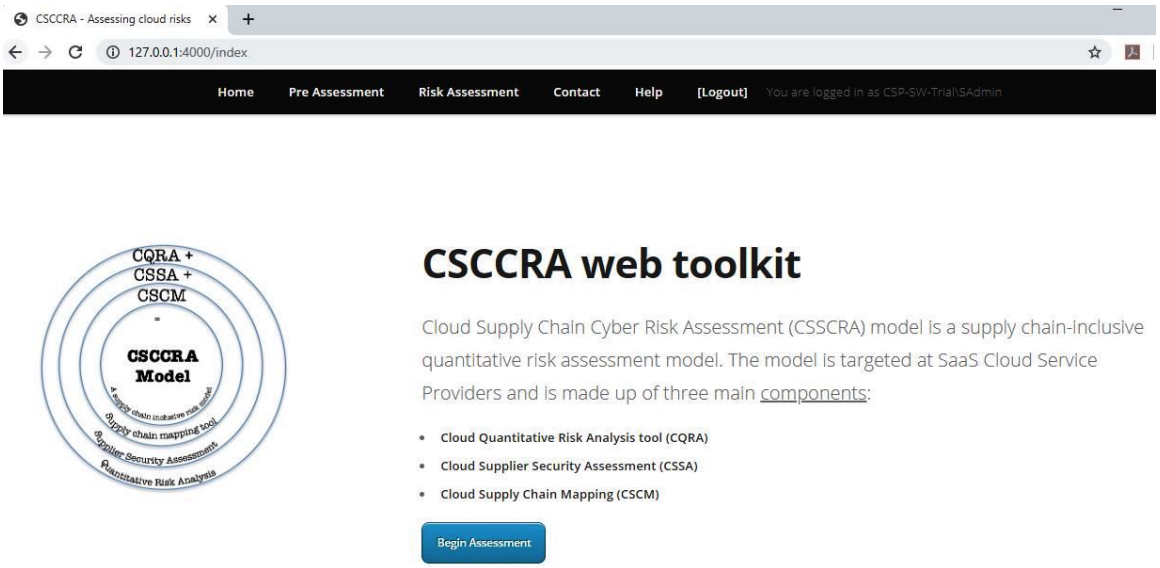


Figure 9.2: Homepage of the CSCCRA web application

```
C:\PyCharm Edu 2018.3\web_20062019\web>.\app.py
 * Serving Flask app "app" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: on
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 231-033-180
 * Running on http://127.0.0.1:4000/ (Press CTRL+C to quit)
```

Figure 9.3: Running the web application from CLI

development of the tool, it provided us with enough information to design and implement the application. During the process, we identified aspects of the risk model that required guidance from the assessor and simplified these operations in the web tool. For example, the concept of estimating the probability of risk event had two considerations (with or without security controls). The case study participants judged these probability estimations as confusing, so in the tool, we limited it to one probability estimate. Another lesson learned from our case studies is about the Monte Carlo simulation using the Palisade @Risk tool. Using the @Risk tool, it took 90secs to run five (5) simulations of 100,000 iterations each. Benchmarking this time against the time expended when the same amount of simulation was done on our code, we realised ours took considerably longer (circa 230secs). Therefore, in keeping with our UX design focus, we reduced the number of iterations, running only 10,000 iterations over three simulations.

The design of the web interface provides users with useful hints on the risk assessment process and nudged them in the right direction, offering user-friendly feedback when a wrong input is entered. The web application has a help page (see Figure 9.4), which explains the CSCCRA risk assessment process and provides a step-by-step guide on how

to complete each phase of the assessment. We leveraged the feedback mechanism (flashing message) integrated into the Flask framework to present users with a message at the end of a request. The application is designed around the needs of users and therefore, is built for human speed. It enables stakeholders within CSPs to collaborate while still going through the risk assessment process at a good pace, presenting them with the result promptly.

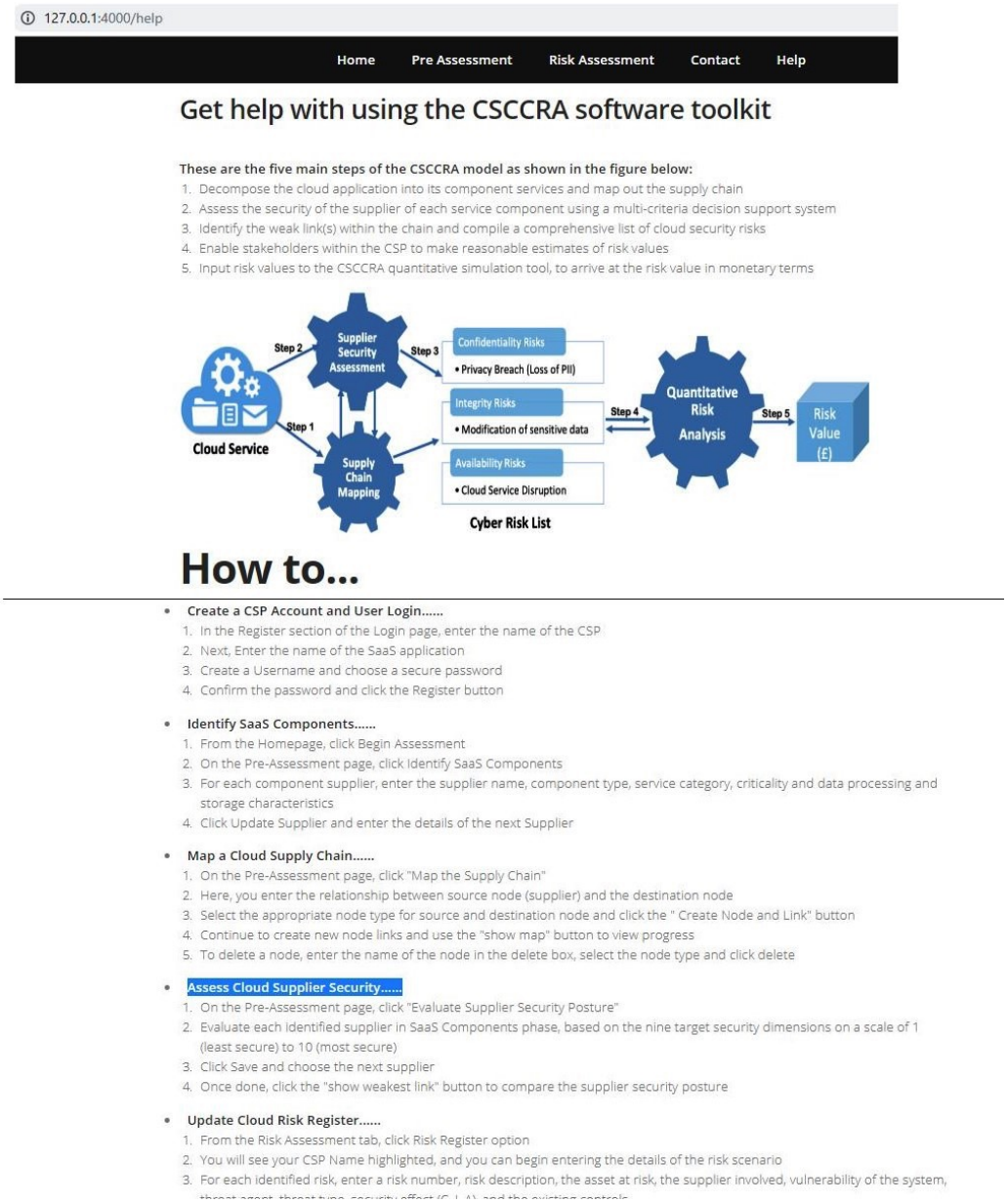


Figure 9.4: User help page for the CSCCRA web application

Lastly, despite the short time the researcher had to implement the tool, we reckon the development of the web application has been a success. However, there exist some limitations. For example, in the course of developing the application, we noticed that the Flask framework had no database abstraction layer, nor does it support form validation. This

meant that we had to write the codes for form validation, which was not ideal. Also, while SQLite supports multiple users, it locks the whole database when writing, which can become an issue when different CSP users make concurrent writes. As we look to migrate the web application to a cloud platform, we need to address these gaps and others that will be identified in the course of the evaluation. In our future iterations, we plan to install extensions for object-relational mapper (ORM), form validation and open authentication. Also, we plan to migrate the application's database to MSSQL or MySQL and use SQLAlchemy for the database abstraction layer to map the database data into python objects.

9.2 System Evaluation

Having validated the applicability of the CSCCRA model to assessing CSP risks in chapters 7 & 8, the evaluation of the web application is to confirm the usefulness, suitability and practicality of the application when used by CSPs to assess their risks. As such, following the development of the CSCCRA web application, we evaluated the tool in two phases. First, we evaluated the application with a focus group made of five computer science and cybersecurity researchers. Secondly, seeing the critical feedback that could be gained from professionals in the field, we evaluated the application within a CSP environment.

9.2.1 Focus Group Evaluation

We evaluated the workings of the web application by demonstrating the risk assessment process to a focus group made up of five computer science and cybersecurity researchers from Oxford University. We gave a brief introduction of the model and the aim of the exercise. We presented the participants with a sample case study, explaining how the model will assess the risk in the given scenario. After this, we got one of the participants to launch the web application and begin the risk assessment of the sample case study with the group, starting with the pre-assessment activities (component identification, supply chain mapping and supplier assessment) before progressing to risk identification and evaluation. We informed the group of the need to reference the help page (see Figure 9.4) should they get stuck on a process and also reach out to the researcher who was on hand to assist. Through the process, we got the participants to discuss their observations and to point out the merits and limitations of the web application.

At the end of the 3-hour activity, we presented the group with a questionnaire to evaluate the web application (see Table 9.1). For each of the evaluation criterion we required the participants to rate the web application on a scale of 1 to 5, where *5 = Outstanding, 4 = Good, 3 = Satisfactory, 2 = Poor and 1 = Unsatisfactory.* The questionnaire asked questions meant to help us gauge how well we met the top five requirements identified in the specification phase (see section 4.4).

Table 9.1: CSCCRA Web Application Evaluation Questionnaire

	Outstanding (score = 5)	**Good (score =4)**	**Satisfactory (score = 3)**	**Poor (score =2)**	**Unsatisfactory (score =1)**
1. The user interface is intuitive and promotes easy navigation					
2. The application handles invalid user input correctly					
3. The application outputs quality data to the user					
4. The application is demonstrably effective for assessing CSP risks					
5. The information provided in the help page is clear, concise, and informative					
6. The risk assessment result is presented in a usable format					
7. The application is practical for CSP environments					
8. The application supports continuous monitoring of CSP risks					
9. The application supports collaboration among CSP stakeholders, including stakeholders with varying abilities and experiences					
10. The web application achieves its purpose					

As shown in Table 9.2, the group feedback confirmed the web application was useful, viable and practical for assessing CSP risks. All the evaluation criterion were rated as satisfactory (3) and above. From a usability perspective, the feedback was positive. Some of the highlighted application benefits, related to its accessibility (browser-based), the understandability of the assessment process and the ease-of-use. Participants acknowledged how each step in the model fed data to the next step and highlighted the progressive nature of the web application. However, the application exhibited some shortcomings during the evaluation, many of which were related to error handling and performance. The participants observed that the application depended on the quality of the input data, and in some cases, did not handle invalid inputs correctly. The group scored the application low on its error handling abilities (mean score of 3.4). We accept the criticism and see it as an area for improvement in future releases. Also, the group identified that the risk analysis module was slow to compute cloud risk value. While we identify the need to improve the simulation time, possibly by leveraging high-performance cloud servers, we drew the attention of the group to the limitation inherent in the @RISK tool, and how we have modified the number of iterations to achieve a balance between accuracy and usability.

Overall, the group's evaluation of the tool judged it to be fit-for-purpose and useful for assessing cloud provider risk. The participants also concluded that the application fulfils the purpose of the CSCCRA model (mean score of 4.2). They identified areas where improvements can be made, such as the layout of the icons, improved graphics, use of placeholder attributes (describing expected values for input fields) and increased speed of computation. While some of the suggestions were immediately implemented, others that require more effort were marked for future releases, when the web application will be migrated to a cloud platform. It is worth noting that we did not evaluate the security of the application. This is because, as of the time of the group evaluation, we had not conducted a web application security test, and are currently not confident of its security. Hence the

Table 9.2: Focus Group Evaluation of the Web Application

No.		**Mean Score**	**Standard Deviation**
1.	The user interface is intuitive and promotes easy navigation	4	0.71
2.	The application handles invalid user input correctly	3.4	0.55
3.	The application outputs quality data to the user	4.4	0.55
4.	The application is demonstrably effective for assessing CSP risks	4.4	0.89
5.	The information provided in the help page is clear, concise, and informative	4.8	0.45
6.	The risk assessment result is presented in a usable format	4	0.71
7.	The application is practical for CSP environments	4.4	0.55
8.	The application supports continuous monitoring of CSP risks	3.8	0.45
9.	The application supports collaboration among CSP stakeholders, including stakeholders with varying abilities and experiences	4.4	0.55
10.	The web application achieves its purpose	4.2	0.84

reason why we limited this evaluation to the functionality, usability and data integrity of the web application.

9.2.2 Case Organisation Evaluation

Seeing that the focus group evaluation was reasonably successful, we progressed to evaluate the model in a real-world environment. While we did not conduct a new case study using the automated tool, we evaluated the usefulness and practicality of the web application with one of our three case organisations (CSP-C). In this evaluation, we got CSP-C to use the application in assessing some of the risks identified in a different case study (see Table 7.4) and later obtained feedback using the questionnaire in Table 9.1. We approached this evaluation in this way because we reasoned that having CSP-C assess the risk of an organisation they were not familiar with, will help them to focus on the workings of the application. Similar to the focus group, each question addressed an evaluation criterion and required each participant to rate the tool on a scale of 1 (Unsatisfactory) to 5 (Outstanding). We followed up the questionnaire with open-ended questions around the web application and how the CSP evaluated its applicability to their environment. Three of the participants who took part in the earlier case study were available for the evaluation.

Ideally, we should have evaluated the web application with a new case organisation, but for the time required to setup a case study and conduct the analysis, we chose to leverage one of our existing case organisation. The opportunity to evaluate the application with CSP-C came when the researcher visited the organisation to present the case study results to the team and discuss the risk treatment suggestions. CSP-C found the case study exercise valuable and were willing to support our bid to make the risk assessment application available to a broader audience. Nevertheless, evaluating the application with one of our

Table 9.3: CSP Evaluation of the Web Application

No.		**Mean Score**	**Standard Deviation**
1.	The user interface is intuitive and promotes easy navigation	4.67	0.58
2.	The application handles invalid user input correctly	4.0	1.00
3.	The application outputs quality data to the user	4.67	0.58
4.	The application is demonstrably effective for assessing CSP risks	4.67	0.58
5.	The information provided in the help page is clear, concise, and informative	5.00	0.00
6.	The risk assessment result is presented in a usable format	4.33	0.58
7.	The application is practical for CSP environments	4.67	0.58
8.	The application supports continuous monitoring of CSP risks	4.00	0.00
9.	The application supports collaboration among CSP stakeholders, including stakeholders with varying abilities and experiences	4.67	0.58
10.	The web application achieves its purpose	4.33	0.58

case organisations turned out to be a sound decision because the participants were already aware of the model based on the workings of its earlier prototype.

To begin the assessment, we provided the participants with a brief description of the application and the refinements we have made to simplify the model based on case study suggestions. We assured the participants that the web application followed the systematic flow of the model and covered all its essential steps. The participants were made aware of the help page and the definition of essential factors which have been provided to ease the use of the web tool and reduce mental fatigue. The researcher notified the participants of our intention to observe them as they used the tool to assess their cloud risks. A more detailed description of how the stakeholders completed each step of the assessment process, including screenshots taken during the evaluation can be found in Appendix E.

At the end of the exercise, the participants completed the evaluation questionnaire (see Table 9.3) and discussed the merits and shortcomings of the application. The participants confirmed the usefulness of the web tool for assessing cloud provider risks and emphasised the importance of CSPs having a web tool that can ease the risk assessment process. One of the participants said, "*with this tool, CSPs no longer have to maintain spreadsheets and documents for their risk assessment*". Another participant mentioned that with the application, ''*CSPs no longer have to share their most sensitive risk information with external assessors, but can input it directly into the tool*''. They identified that the web application gives CSPs the ability to monitor and update their security risks continuously. They reckoned that with a few clicks, CSPs can update their risk register or supply chain map, assess the influence of a supplier change on the SaaS's security posture and estimate their cloud risks. The participants highlighted the contrast between the manual process where only the researcher had access to the integrated but disjointed prototype tool, and the current situation where the CSP themselves are driving the risk assessment process, with little

assistance from the researcher.

Similar to the focus group, the participants found the information contained in the application's help page clear and concise and one of them said, *"I should be able to run through the process without any assistance, based on the information in the help page"*. We take this as a compliment but look forward to addressing the shortcomings identified in both evaluations before migrating the tool to the cloud. The shortcomings identified during this evaluation were similar to those already identified in the focus group evaluation. Other areas where the participants suggested improvement include providing CSPs with a view of the risk register before risk factor evaluation, reducing data input by allowing experts re-use/edit their past estimations, improve graphics and enable support for multi-user login. We welcome their suggestions and hope to make the changes to the application in our future releases.

Lastly, based on the preceding paragraphs and sections, it can be concluded that in the context of these evaluations, there is significant support for the CSCCRA web application. While we look to improve the UX, design, security and performance of the application, this support confirms the applicability and practicality of the application to assessing CSP risks. In conclusion, this evaluation validates the CSCCRA's inclusive, structured and systematic approach to cloud risk assessment, and its ability to assist CSPs in delivering objective risk results.

9.3 Summary

In this chapter, we completed a two-stage evaluation of the CSCCRA web application. First, we demonstrated the application within a focus group setting, after which we got a real-world CSP to use the application in assessing cloud risks. Acknowledging that the application might not pass the scrutiny of automated and quantitative evaluation strategies such as Web Quality Evaluation Method (WebQEM) [228], our elementary but structured evaluations, confirmed the usefulness, suitability, practicality and quality of the CSCCRA web application.

Our implementation met the requirements identified in the specification and design phase and was judged by the participants to be intuitive, understandable and reliable, with no apparent issues such as broken links or orphan pages. They found the help pages useful, providing them with the required information on how to complete the assessment. However, despite the application being appraised to be practical and applicable to the cloud industry, there were some limitations, particularly around its performance and user experience. From what we observed, these shortcomings were not viewed as factors that undermined the usefulness of the application and we hope to improve on these factors in future releases.

Chapter 10

Conclusion

10.1 Introduction

A key goal of this thesis was the investigation of the effect of supply chain transparency on cloud risk assessment. We broke this goal down into four phases, including the validation of the supply chain transparency and risk assessment gaps, the proposal of a risk assessment model to address some of the gaps and the evaluation of the proposed model. Having accomplished our goal, this chapter ends the thesis by presenting project conclusions, limitations of the study and directions for future work.

10.2 Conclusions and Discussion

In concluding this research project, we must begin by assessing the achievement of our original aims and objectives. This research which was motivated by a series of cloud service outages in 2016 & 2017, set out in Chapter 1 to address the following research goals:

- Establish a theoretical foundation for the study regarding cloud supply chain transparency and its effect on cloud risk assessment;
- Validate the existence of cloud supply chain gaps with industry practitioners;
- Propose a risk assessment model that addresses the supply chain transparency gaps;
- Validate and improve the proposed model, including implementing the model as a web-based software.

Our central query was as follows: *Can the transparency of the supply chain improve the objectivity of cloud risk assessment?* We tackled this central objective by posing four key research questions (RQ), and we believe each question has been addressed in the previous chapters of this thesis. We explored the potential of a quantitative and supply chain-inclusive approach to assessing cloud provisioning risks within SaaS environments and based

on our results confirmed the applicability of our approach. While there are previous studies on cloud provisioning risk assessment, as shown in Section 3.2, to the best of our knowledge, CSCCRA is the first quantitative cloud risk assessment model that addresses the effect of the supply chain transparency on cloud risks. We established through numerous investigations that our approach, which admittedly increases the rigour involved in the risk assessment process, also enhances the objectivity, repeatability and reproducibility of the assessment results.

To summarise our project, we begin with our initial study (survey and interview) with industry experts on the effect of transparency on cloud supply chain risks (Chapters 4 & 5). Before conducting this study, our review of the literature showed that little attention was paid to the supply chain as a source of cloud risks. The result of this study confirmed that cloud stakeholders had limited visibility or awareness of their third party risks and established how the visibility had hindered them from adequately assessing their risks **(RQ1.1)**. The study acknowledged the role cloud transparency, particularly the visibility of security controls and processes, played in improving customer confidence in cloud services and reducing perceived risk. It went on to suggest transparency features which cloud providers should be willing to share with their customers.

As a follow up to the study and to assess if current risk assessment methods adequately assessed cloud supply chain risks, we conducted another survey with cloud providers and customers **(RQ1.2)**. This survey was to understand the industry practices with regards to cloud risk assessment and to gauge the participants level of awareness of cyber supply chain risks. The evidence from the survey suggested that the current industry approaches were unable to address the dynamic risks of the cloud, which involves the more extensive supply chain. With limited visibility of security controls across the supply chain, stakeholders conducted their cloud risk assessments at yearly intervals and employed the use of traditional (qualitative) methods, which are subjective in their assessment of the Target of Assessment (ToA). We concluded that due to the potential multiplicity of actors and the evolving nature of cloud risks, conducting static one-time risk assessments which concentrates on the focal organisation can no longer suffice.

Given the scarcity of initiatives for the practical implementation of a quantitative risk assessment model, we proposed the CSCCRA model, a quantitative and supply chain-inclusive approach to assessing cloud risks (Chapter 6). The scope of the project was also reduced to assessing cloud provisioning risks within SaaS CSP environments. We chose to investigate the impact of the model on cloud providers first because we identified the advantage CSPs have over their customers concerning supply chain transparency and visibility of security controls. Despite the often-cited concerns about quantitative risk models [32, 167], implementing the CSCCRA model as a quantitative model was more applicable to our research,

not least because of its use of a rigorous process which allows for a deeper understanding of the interconnectedness of cloud risks. Being an inclusive and business-aware model, assessing risks using the CSCCRA model facilitates a situation where stakeholders (business and technical) from different arms of the CSP organisation contributes to the comprehensive understanding of the cloud risks coherently. Likewise, quantifying cloud risks in monetary terms also helps to move the economic implications of cloud risks from a compartmentalised technical issue into a business issue [261].

Building on the systems thinking principle of the *whole being more than the sum of its parts*, the CSCCRA model assesses CSP cloud risk, not based on the risk of individual components in isolation, but by understanding the interactions, dependencies and relationships that are involved in the delivery of the service. We proposed the need for CSPs to analyse the complete path of the SaaS application flow, verify the security posture of suppliers and identify the blind spots in the supply chain, leaving very little room for assumptions. As such, the model requires the CSP to be aware of the logical and physical dependencies they have on their supply chain. The cloud supply chain mapping (CSCM) component helps CSPs to detect convergence risks by visualising information flow through critical suppliers. The CSCM is also implemented as an asset management tool and is fundamental to incorporating good IT governance to CSP environments.

Furthermore, the model requires the CSP to be aware of their supplier processes, evaluate supplier security controls and identify weak spots in the supply chain. For this, we introduced the cloud supplier security assessment (CSSA) tool, a supplier rating service into the CSCCRA model. The CSSA tool works on the premise that *security can only be as effective as the weakest in the chain from end-to-end*. To identify the reliability and security factors cloud providers can use in evaluating suppliers **(RQ2)**, we engaged in a Delphi study. The Delphi study achieved consensus on a total of 52 security criteria grouped into nine target security dimensions, many of which corresponded to security measures included in recognised security standards and control sets such as ISO/IEC 27001/2, NIST SP 800-53 and COBIT v5 (see Appendix B).

Following the development of the CSCCRA model, we completed a three-staged evaluation process to validate the usefulness and applicability of our proposed model in assessing cloud provider risks. We conducted an *Author Evaluation*, *Domain Expert Evaluation* (see Section 6.6) and culminated it with a *Case Study Evaluation* (Chapter 7). Also, we systematically evaluated the model with three other conceptual models proposed for cloud provisioning risks (see Section 6.8) and carried out a completeness comparison of our model with other established risk assessment standards (see Section 6.7). The evaluations confirmed the functional improvements of the CSCCRA model on the existing conceptual and traditional risk frameworks. The novelty of the model to expand its functional scope to

include the supply chain also played an integral part in its success. The CSSCRA approach helps CSP address some of the common challenges of the complex 21st century organisation [138], e.g. identify and assess cloud suppliers, expose areas of weakness, assist CSP to prioritise risks based on the level of exposure.

The empirical findings from our in-depth case study evaluation of the model with three SaaS CSPs (Chapter 8), confirmed the usefulness and applicability of the model to CSP environments. According to the case organisations, the components of the CSCCRA model provide CSPs with an insightful view of their supply chain risks. The CSCM simplified the presentation of complex supply chain information using maps, while the CSSA brought transparency to the security posture assessment of cloud suppliers, providing a quantitative measurement of security performance across the chain. The pre-assessment tools (CSSA and CSCM), provided stakeholders with the *"big picture"* of their threat landscape, with this increasing their objectivity during the risk assessment process and the justifiability of cloud risk assessment results **(RQ3)**. Both tools addressed the clouds' insufficient due diligence challenge [208], by increasing visibility into the security controls of cloud suppliers. They complemented the risk assessment process and improved CSPs understanding of their cloud risks, although, produced more tangible results in the identification of operational and infrastructural security risks.

The entire risk assessment process fostered collaborative communication among the stakeholders, which was judged to be more advantageous when compared to the siloed approach of traditional risk assessments. The participants acknowledged the flexibility of the model to address different SaaS CSP needs, including but not limited to, continuous risk assessment, redesign of cloud architecture, supplier selection and cost-benefit analysis of mitigating security controls. The model's supply chain inclusivity and ability to present the value of risk in monetary terms, owing to its quantitative approach, was said to have bridged some of the existing cloud risk assessment gaps.

Acknowledging that practitioners have long claimed that success in risk assessment can only be achieved by the application of a systematic and robust approach [259], our application of the CSCCRA model to assessing cloud risks confirms this claim. The case study participants affirmed that the model follows a systematic, structured, transparent, responsive and inclusive approach to risk assessment. The results of the case study risk assessment show that the model improves human judgement on security risks, by applying techniques such as calibration, subjectivity probability, collaboration and decomposition of factors [143]. However, we recognise there is still room for improvement, seeing that stakeholder's estimation of their asset and impact cost still show signs of extreme subjectivity. Despite the imperfections, the three case organisations, who were more acquainted with the qualitative risk assessment methods (e.g. ISO/IEC 27001), were willing to continue using

the model to assess their cloud risks. This singular gesture supports the advantage of our approach. Comparing the CSCCRA to an existing qualitative method (see Section 7.3), we realised that the ability of the model to decompose a cloud risk data into a clear, observable and useful format and present the risk value in monetary terms, was found to promote cost-effective risk mitigation, optimal risk prioritisation and improved decision-making **(RQ4)**. The study also confirmed that the application of mathematical operations to cloud risk assessment promotes transparency.

While assessing cloud risks remains a challenge to the cloud industry at large, and visibility of security controls remains a leading inhibitor to cloud adoption [74], the results of this research provide evidence to motivate the need for increased security transparency by cloud providers [150]. The CSCCRA model contributes a Risk Assessment as a Service (RAaaS) solution to the cloud industry, which, according to Marianthi et al. [309], is an open research issue. We satisfied two of the three requirements for implementing RAaaS: continuous collection of accurate data, and comprehensive qualitative and quantitative metrics targeted to the cloud environment. While we do not have an established knowledge-base of available public information, or a method for accumulating this automatically, our current approach which feeds into a modelling tool partially fulfils the third requirement. We achieved our final research aim of developing the model into a web-based application that can be used for the continuous assessment of cloud provision risks, where the tool considers the cybersecurity posture of the broader supply chain in its estimation of risk factors and resultant risk value (see Chapter 9). Refusing to stop at the conceptual stage, we evaluated the effectiveness of the developed web application with a focus group and a case organisation. Both evaluations appraised the web application as being practical and applicable to the cloud industry, despite its limitations.

Lastly, while we understand that the uniqueness of our approach to addressing cloud risk assessment gaps could be seen in some quarters as a break away from the norm and could be scrutinised for that purpose, our model validation with industry experts and three SaaS organisations has shown the capability of our model to outperform existing methods. The case study results have validated the robustness, usefulness, reproducibility and practicality of our model even within the cloud industry. However with the cloud industry proliferated with qualitative methods, and cloud stakeholders mainly seeing risk assessment as a compliance requirement instead of a business enhancer, it might take a while for the CSCCRA to gain mainstream attention. Nevertheless, we aim to continue pushing research boundaries and promoting the merits of a supply chain-inclusive approach to cloud risk assessment.

10.3 Limitations

Having undertaken mixed-method research to address our research questions, we, in this section, identify some of the limitations of our work. Each of the qualitative and quantitative study undertaken, i.e. survey, interviews, Delphi study and case study, had their shortcomings and influences that restricted our methodology. We have discussed the limitations specific to each study in their respective chapters, but here, we critically reflect on the combined work to recognise areas that might have influenced our conclusions. While the limitations, common to similar studies, i.e. small sample size and lack of generalisability, were evident in this work, our application of scientific rigour throughout the research process was instrumental to its success.

We begin with the initial survey conducted in Chapter 5 to validate the supply chain transparency gap in the cloud industry. Seeing that the strength of survey research is in its cost-effectiveness, reliability and versatility, our study was limited due to its small sample size. While our case study scenario-based survey elicited quality responses from the cloud stakeholders and we were able to follow-up the participants by conducting semi-structured interviews, the findings are less generalisable to the cloud industry. The study was limited to a small pool of experts, who were willing to take part despite their busy schedule during a cloud exhibition in 2016. Also, it appears that those who participated were interested in the subject, which might have skewed the sample. However, we feel that our combination of qualitative and quantitative methods captured a more complete and holistic portrayal of the existing transparency gap and identified basic transparency features to bridge the information asymmetry between cloud providers and customers. Nevertheless, we see an opportunity for future research to be conducted in this area, where a researcher with access to a large pool of cloud experts spread across multiple countries, replicates the study to validate our findings.

According to Scrimshaw & Gleason [277], survey methods are a useful tool in collecting objective data, but weak in collecting subjective and attitudinal data. Because our next study was targeted at understanding the industry practices with regards to cloud risk assessment and stakeholder's level of awareness of cyber supply chain risks, we relied on the broad capability of the survey method. Although we had a larger sample size (N= 62) compared to our initial survey, we cannot guarantee the accuracy and honesty of the answers provided by the respondents, as some of the questions probed the internal risk assessment practices within the respondent's organisation. Despite the anonymity of the reporting process, we are aware that respondents might consciously or unconsciously want their organisation to look good from the outside, more so as it related to security. Nevertheless, our opinion is that the majority of the respondents were genuine, and their high internal consistency score supports our viewpoint.

Thirdly, in our conduct of the Delphi study to identify security factors for cloud supplier assessment, we adhered to rigorous guidelines suggested by Okoli and Pawlowski [226] in the design of the study and selection of its participants. Nevertheless, we acknowledge the possibility of unintentional researcher bias. Critically reflecting on the process, we are uncertain if the invitation letter sent out to a broad audience of cloud stakeholders negatively impacted the quality of the respondents, or if the initial case study-based questionnaire influenced the participants. To avoid these occurrences, we had before the study, field-tested the questionnaire with experts and academics, but can not rule out the researcher bias. We also avoided getting involved in the process and refrained from imposing our preconceptions on the participants, especially when presenting the summary of the results. However, we were surprised to discover that many of the identified security corresponded with security measures included in recognised security standards and control sets such as ISO/IEC 27001/2 [153], NIST SP 800-53 [221] and COBIT v5 [147]. Our approach also resulted in low panel attrition, since the participants who took part were interested in the study and its result. Notwithstanding, seeing that the security of the cloud is subjective and that the identified security factors are based on the perceptions and opinions of a limited number of cloud experts, the findings of this study, can not be considered as an exhaustive list of security criteria for cloud supplier assessment. Besides, while we followed a rigorous process to reach consensus on the nine target dimensions, we encourage CSPs to be discrete in deciding which of the criteria to apply to their cloud risk assessment exercise.

Moving on to the case studies conducted in Chapter 7 to validate our proposed model, we were limited by the location (UK) and service of cloud provider (SaaS). Despite our efforts at getting well-established cloud providers, we got the impression that they did not see the value-add of our conceptual model since they were already compliant with international standards. Also, due to the in-depth nature of the process, we could not conduct the research on a large scale, which might have provided us with the possibility of generalising the result. The CSPs, did not have comprehensive knowledge of their supply chain or supplier processes, nor did they have a recent vulnerability assessment of their cloud service, and both circumstances increased the subjectivity of their estimations and the overall result of the assessment. Another limitation of the study was our inability to carry out an in-depth comparison of the CSCCRA with other conceptual cloud risk assessment model, as this was judged by the CSPs to be time-consuming. Future research work might explore this path, should the necessary resources be available to the research team. Risk assessments are not expected to be perfect, mainly because the data upon which they are built are often inaccurate. However, the results of the case studies confirm that our approach was judged to be suitable, sufficient and practical for assessing cloud provider risks. Our initial findings were convincing, and the implementation and evaluation of the

developed CSCCRA web application also demonstrated the usefulness and applicability of the model to assessing CSP risks.

Overall, we accept the limitations posed by our methodology. However, despite the limitations of this multi-staged research work, to the best of our knowledge, this study is the first one to consider cloud risk assessment from a supply chain perspective comprehensively. Our rigorous approach to cloud risk assessment combines aspects of various disciplines, ranging from cybersecurity, supplier assessment, systems thinking, decision support systems, transparency, supply chain mapping and quantitative risk assessment to address a cloud provider need. Also, the findings of this study offer several directions for extending the knowledge-base in the domain of cloud computing and risk assessment.

10.4 Directions for Future Research

Based on the research reported in this thesis, there are various exciting avenues for future research, and in this section, we discuss some of the relevant ones.

Information security risk in the cloud has remained a cross-cutting concern for cloud consumers and providers, seeing that it integrates other factors such as trust, transparency, accountability and cost. The importance of assessing cloud risks has mainly been motivated by the dynamic context in which the services and application are implemented. However, due to the proliferation of the traditional methodologies applied to assess cloud risks, it would seem that cloud risks are ever-increasing. Furthermore, most organisations, due to their resource constraint, fail to conduct due diligence on their third and fourth-party vendors, even though there is an ever-increasing dependence on these vendors. They implement point in time analysis following an incident, or periodic assessment for compliance purposes.

According to Bellandi et al. [38], the stalemate around the research on qualitative risk assessments techniques has given room for the development of novel quantitative models. However, building these models on unreliable data or subjective expert guesses will not improve the status quo. As such, there is a need for more work around cloud incident reporting and supply chain transparency. We anticipate the need for technology-enabled automation and proactive solutions in addressing the need for continuous risk assessment in the cloud. The cloud is amenable to automated risk assessment and mitigation, where the members of its supply chain can be dynamically monitored for risk and vulnerabilities within their system, and the risks remediated before getting exploited by attackers. This process can include scanning for change in supplier configuration or software code, which triggers an alert for a new risk assessment or potential remediation if applicable.

Due to the numerous indirect assets involved in the provision of cloud services, research should be conducted on how best CSPs can proactively assess the risk of dealing with all known suppliers to allow them to identify their limitations and improve their performance.

The application of a dynamic and flexible risk assessment model which adequately identifies and manages cloud risks based on the context of the environment could be productive. New cloud models should factor in the interdependence and complexity of individual components that make up the cloud service, including the impact of indirect assets in the risk assessment process. This approach involves the application of structural analysis of the cloud environment and application of data-driven evidence through the stages of a cloud assessment.

Therefore, a way to extend the CSCCRA model's supply chain mapping approach will be to improve the CSCM so it can generate quantitative measures that characterise the structure of the cloud supply chain. While the visual representation of the cloud supply chain remains a useful method for conveying complex dependency information, there is a need for stakeholders to understand the elements and linkages in their integrated network ecosystem through quantitative analysis. There is also a need for the CSP to be able to measure the indirect costs of failures within their supply chain. Moreso, seeing that a risk event is often assumed to be linked to direct suppliers, whereas, in reality, it could propagate over different levels, there is a need to simulate various risk scenarios using network analysis. This analysis enables the CSP to capture risk propagation phenomenon beyond the first-tier.

Furthermore, while the causes of cybersecurity incidents may be technical, their effects are purely business, with impacts on the reputation and continued viability of the CSP. Therefore, proposals for cloud risk assessment models should look towards quantitative risk methodologies that enable them present cloud risks based on its impact to the business (i.e. loss of business or cost to recover), factoring the value of the asset into the risk estimations. According to some authors, asset characterisation and valuation, which should be considered as crucial components of cloud security risks assessment, have not been well discussed in the existing frameworks [313]. With this in mind, we suggest new models should embrace quantitative methods in assessing cloud risks and present the risk value as an actual dollar amount; an approach which is gradually gaining momentum within the cloud industry. Our research has also provided incentives to strengthen this proposal, and we acknowledge its potential for improving the quality of cloud risk assessment.

Lastly, researchers and practitioners within the cloud community should strive to develop assessment tools targeted at cloud provisioning risks, which are both useful for science and practice. This enables CSPs to deal effectively with the risks involved in the design, deployment, configuration, or operation of the cloud. Also, we anticipate that this will improve the agility and reliability of cloud services, helping CSPs to handle predicted and unforeseen changes, while also assisting them in meeting their SLAs. Additionally, researchers should endeavour to implement their proposed models, to measure its capability and assure its effectiveness in addressing the cloud risk assessment challenges.

10.5 Concluding Remarks

This work has explored the effect of supply chain transparency on cloud risk assessment. While insufficient due diligence among cloud stakeholders continues to be a significant hindrance to comprehensive risk assessment [208], our application of the systems thinking approach to the problem area, provided a more suitable context for CSPs to assess their interconnected cloud risks. The research showed that CSPs awareness of supplier processes and security controls together with increased visibility into the vulnerability of the chain, helps to foresee challenges and enable a proactive response to resulting threats.

Following our validation of the importance of supplier transparency in the conduct of objective and comprehensive cloud risk assessment, we indicate that the time is right for Government legislation to be made to promote cloud supply chain transparency. We believe that if the fundamentals of initiatives such as the United State's Cyber Supply Chain Management and Transparency Act of 2014 [260] are applied to cloud computing, the cloud will be more secure and its adoption rate will improve. Consequently, this will ensure stakeholders are aware of the possible vulnerabilities in the supply chain and the capability of their provider's security controls to address existing gaps.

Taken together, this study provides support for two high-level conclusions. Firstly, the time is now right for quantitative cloud risk assessment models. Our research has shown that applying a systematic, structured, transparent and supply chain-inclusive approach to cloud risk assessment can yield meaningful risk values and support proactive risk mitigation. Secondly, the call for cloud supply chain transparency is here to stay. Therefore, CSPs need to be aware of their logical and physical dependencies on the supply chain, understand their supplier processes, and be more transparent with their customers about the security controls employed to protect their most sensitive data.

Bibliography

[1] Imad Abbadi and John Lyle. Challenges for provenance in cloud computing. *USENIX Workshop on the Theory and Practice of Provenance (TaPP'11).*, 2011.

[2] Imad M. Abbadi. Clouds' infrastructure taxonomy, properties, and management services. *Communications in Computer and Information Science*, 193 CCIS(PART 4):406–420, 2011.

[3] Robert Abbott and Mirsad Hadžikadić. Complex adaptive systems, systems thinking, and agent-based modeling. In *Advanced technologies, systems, and applications*, pages 1–8. Springer, 2017.

[4] Raghavendra Achar and P. Santhi Thilagam. A broker based approach for cloud provider selection. *Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2014*, pages 1252–1257, 2014.

[5] Tobias Ackermann, André Miede, Peter Buxmann, and Ralf Seinmetz. Taxonomy of Technological IT Outsourcing Risks : Support for Risk Identification and Quantification. *European Conference on Information Systems (ECIS)*, (June):1–16, 2011.

[6] Vineet Agarwal and Richard J. Taffler. Twenty-five years of the Taffler z-score model: Does it really have predictive ability? *Accounting and Business Research*, 37(4):285–300, 2007.

[7] Naim Ahmad. Cloud computing: Technology, security issues and solutions. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pages 30–35, 2017.

[8] AJ. Miniport — HTML5 UP. `https://html5up.net/miniport`. (Accessed April 28, 2019).

[9] Olusola Akinrolabu, Ioannis Agrafiotis, and Arnau Erola. The challenge of detecting sophisticated attacks: Insights from soc analysts. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, pages 55:1–55:9, Hamburg, Germany, 2018. ACM.

[10] Olusola Akinrolabu, Andrew Martin, and Steve New. Assessing cloud risk: The supply chain perspective. `https://www.bcs.org/content/conWebDoc/59876`, 2018.

[11] Olusola Akinrolabu and Steve New. Can Improved Transparency Reduce Supply Chain Risks in Cloud Computing. *Proceedings of the 7th International Conference on Operations and Supply Chain Management (OSCM)*, 10(3):130–140, 2016.

[12] Olusola Akinrolabu, Steve New, and Andrew Martin. Cloud Service Supplier Assessment : A Delphi Study. In *Proceedings of the Eighth International Conference on Innovative Computing Technology (INTECH),2018, Luton, UK*, pages 142–150, 2018.

[13] Olusola Akinrolabu, Steve New, and Andrew Martin. CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. In *European, Mediterranean, and Middle Eastern Conference on Information Systems*, pages 177–184. Springer, 2018.

[14] Olusola Akinrolabu, Steve New, and Andrew Martin. Cyber supply chain risks in cloud computing - bridging the risk assessment gap. *Open Journal of Cloud Computing (OJCC)*, 5(1):1–19, 2018.

[15] Olusola Akinrolabu, Steve New, and Andrew Martin. Assessing the security risks of multicloud saas applications: A real-world case study. In *2019 IEEE 6th International Conference on Cyber Security and Cloud Computing (CSCloud)*, pages 81–88. IEEE, 2019.

[16] Olusola Akinrolabu, Steve New, and Andrew Martin. CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. *Computers Journal*, 8(3):1–17, 2019.

[17] Olusola Akinrolabu, Jason R C Nurse, Andrew Martin, and Steve New. Cyber risk assessment in cloud provider environments : Current models and future needs. *Computers & Security*, 87:101600, 2019.

[18] Henk Akkermans, Paul Bogerd, and Jan Van Doremalen. Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics. In *European Journal of Operational Research*, volume 153, pages 445–456, 2004.

[19] Sameer Hasan Albakri, Bharanidharan Shanmugam, Ganthan Narayana Samy, Norbik Bashah Idris, and Azuan Ahmed. Security risk assessment framework for cloud computing environments. *Security and Communication Networks*, 7(11):2114–2124, 2014.

[20] Adel Alkhalil, Reza Sahandi, and David John. A decision process model to support migration to cloud computing. *International Journal of Business Information Systems*, 24(1):102–126, 2016.

[21] Edward I Altman, Małgorzata Iwanicz-Drozdowska, Erkki K Laitinen, and Arto Suvas. Financial distress prediction in an international context: A review and empirical analysis of altman's z-score model. *Journal of International Financial Management & Accounting*, 28(2):131–171, 2017.

[22] Fatimah M Alturkistani and Ahmed Z Emam. A Review of Security Risk Assessment Methods in Cloud Computing. In *New Perspectives in Information Systems and Technologies*, volume 1, pages 443–453, 2014.

[23] Michael Armbrust, Ion Stoica, Matei Zaharia, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, and Ariel Rabkin. A view of cloud computing. *Communications of the ACM*, 53(4):50, 2010.

[24] Ross D Arnold and Jon P Wade. A definition of systems thinking: a systems approach. *Procedia Computer Science*, 44:669–678, 2015.

[25] Warwick Ashford. Transparency, not security, is biggest cloud challenge. `http://www.computerweekly.com/news/2240185187/Transparency-not-security-is-biggest-cloud-challenge-says-Verizon`, 2016. (Accessed May 01, 2016).

[26] BA Benoit A Aubert, Sylvie Dussault, Michel Patry, and Suzanne Rivard. Managing the risk of IT outsourcing. *System Sciences, 1999. ...*, 00(c):1–11, 1999.

[27] Robert M Axelrod and Michael D Cohen. *Harnessing complexity: organizational implications of a scientific frontier*. New York: Free Press, 1999.

[28] M Azuwa, Rabiah Ahmad, Shahrin Sahib, and Solahuddin Shamsuddin. Technical security metrics model in compliance with iso/iec 27001 standard. *International Journal of Cyber-Security and Digital Forensics*, 1(4):280–288, 2012.

[29] Lee Badger, Robert Patt-corner, and Jeff Voas. Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 800(146):81, 2012.

[30] Youakim Badr and Jean Stephan. Security And Risk Management in Supply Chains. *Journal of Information Assurance and Security*, 2:288–296, 2007.

[31] Nadya Bartol. Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines. *Technovation*, 34(7):354–361, 2014.

[32] Mohammed A Bashir and Nicolas Christin. Three Case Studies in Quantitative Information Risk Analysis. *Proceedings of the CERT/SEI Business Case Workshop: Making the Business Case for Software Assurance*, pages 77–86, 2008.

[33] Srijita Basu, Anirban Sengupta, and Chandan Mazumdar. A quantitative methodology for cloud security risk assessment. In *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, pages 92–103, 2017.

[34] Christian Baun, Marcel Kunze, Jens Nimis, and Stefan Tai. Cloud Computing. *Massachusetts Intitute of Technology*, (January):1–81, 2011.

[35] Business Centric Services Group (BCSG). The small business revolution: trends in SMB cloud adoption. page 23, 2015.

[36] Eloise Beatson. How to Manage Third-Party Risk. `https://blogs.infosecurityeurope.com/how-to-manage-third-party-risk/`. (Accessed September 27, 2018).

[37] Jeffrey M. Beck, Wei Ji Ma, Roozbeh Kiani, Tim Hanks, Anne K. Churchland, Jamie Roitman, Michael N. Shadlen, Peter E. Latham, and Alexandre Pouget. Probabilistic Population Codes for Bayesian Decision Making. *Neuron*, 60(6):1142–1152, 2008.

[38] Valerio Bellandi, Stelvio Cimato, Ernesto Damiani, Gabriele Gianini, and Antonio Zilli. Toward economic-aware risk assessment on the cloud. *IEEE Security and Privacy*, 2015.

[39] Wouter Belmans and Uwe Lambrette. The Cloud Value Chain Exposed: Key Takeaways for Network Service The Cloud Value Chain Exposed Key Takeaways for Network Service Providers. pages 1–22, 2012. (Accessed September 18, 2018).

[40] Izak Benbasat, David K Goldstein, and Melissa Mead. The case research strategy in studies of information systems. *MIS quarterly*, pages 369–386, 1987.

[41] Jarg Bergold and Stefan Thomas. Participatory research methods: A methodological approach in motion. *Historical Social Research/Historische Sozialforschung*, pages 191–222, 2012.

[42] Peter L Bernstein. Have we replaced old-world superstitions with a dangerous reliance on numbers. *Harvard Business Review Mar-Apr*, pages 47–51, 1996.

[43] Pim Bilderbeek. Cloudscape United Kingdom. (February):2014, 2014.

[44] Sören Bleikertz, Toni Mastelić, Wolter Pieters, Sebastian Pape, and Trajce Dimkov. Defining the cloud battlefield: Supporting security assessments by cloud customers. *Proceedings of the IEEE International Conference on Cloud Engineering, IC2E 2013*, pages 78–87, 2013.

[45] Markus Böhm and Christoph Riedl. Towards a Cloud Computing Value Network. *GI Jahrestagung Informatik 2010, Workshop: Neue Wertschöpfungsmodelle und Dienste durch Cloud Computing*, pages 129–140, 2010.

[46] Rok Bojanc. Quantitative Model for Information Security Risk. *Engineering Management Journal*, 25(2):267–275, 2013.

[47] Jared Bourgeois, Laura Pugmire, Keara Stevenson, Nathan Swanson, and Benjamin Swanson. The delphi method: A qualitative means to a better future. *URL: http://www. freequality. org/documents/knowledge/Delphimethod. pdf (Citirano 2. 11. 2011)*, 2006. (Accessed May 25, 2018).

[48] Jon M. Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Special publication*, 2015.

[49] Sandor Boyson. Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems. *Technovation*, 34(7):342–353, 2014.

[50] Sandor Boyson, Thomas Corsi, and Hart Rossman. Building a cyber supply chain assurance reference model. *Science Applications International Corporation (SAIC)*, 2009.

[51] Egon Brunswik. Representative design and probabilistic theory in a functional psychology. *The essential Brunswik*, pages 135–155, 2001.

[52] BuiltWith. BuiltWith Technology Lookup. `https://builtwith.com/`, 2018 (Accessed October 12, 2018).

[53] Emil Burtescu. Decision Assistance in Risk Assessment - Monte Carlo Simulations. *Informatica Economic vol. 16*, 16(4):86–93, 2012.

[54] Jerry Busby, Lucie Langer, Marcus Schöller, Noor Shirazi, Paul Smith, and AIT. SEcure Cloud computing for CRitical infrastructure IT, "Methodology for Risk Assessment and Management". *SECCRIT Consortium*, 3(5):1–92, 2014.

[55] Cabinet Office and National Ssecurity and Intelligence. Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019 - A report to the National Security Adviser of the United Kingdom. 2000(March):46, 2019.

[56] Daniele Catteddu, Hogbben Giles, Haeberlen Thomas, and Lionel Dupre. Cloud Computing: Benefits, Risks and Recommendations for Information Security. *Computing*, 72(1):17–17, 2010.

[57] Erdal Cayirci. Models for cloud risk assessment: A tutorial. In Massimo Felici and Carmen Fernández-Gago, editors, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 8937, chapter Models for, pages 154–184. Springer International Publishing, Cham, 2015.

[58] Erdal Cayirci, Alexandr Garaga, Anderson Santana, and Yves Roudier. A cloud adoption risk assessment model. In *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, pages 908–913. IEEE, 2014.

[59] Warren Chan, Eugene Leung, and Heidi Pili. Enterprise risk management for cloud computing. *Committee of Sponsoring Organizations of the Treadway Commission*, page 4, 2012.

[60] She-I Chang, David C Yen, Celeste See-Pui Ng, and Wei-Ting Chang. An analysis of it/is outsourcing provider selection for small-and medium-sized enterprises in taiwan. *Information & Management*, 49(5):199–209, 2012.

[61] Scott Charney and Eric T Werner. Cyber Supply Chain Risk Management:Toward a Global Vision of Transparency and Trust. *Microsoft Corporation paper*, pages 6–8, 2011.

[62] Chi-An Chih and Yu-Lun Huang. An adjustable risk assessment method for a cloud system. In *Software Quality, Reliability and Security-Companion (QRS-C), 2015 IEEE International Conference on*, pages 115–120. IEEE, 2015.

[63] Charles West Churchman and C West Churchman. *The systems approach*, volume 1. Dell New York, 1968.

[64] Paul Cilliers. *Complexity and postmodernism: Understanding complex systems*. Routledge, 2002.

[65] Robert T Clemen and Robert L Winkler. Combining probability distributions from experts in risk analysis. *Risk analysis*, 19(2):187–203, 1999.

[66] Cloud Industry Forum. White Paper 20 - Cloud: Driving Business Transformation. (20):31, 2017.

[67] Cloud Security Alliance. The Treacherous 12 Cloud Computing Top Threats in 2016. *Security*, (February):1–34, 2016.

[68] Michael Cobb. API security: How to ensure secure API use in the enterprise. `http://searchsecurity.techtarget.com/tip/API-security-How-to-ensure-secure-API-use-in-the-enterprise`, 2014. (Accessed January 12, 2019).

[69] Louis Columbus. Roundup Of Small & Medium Business Cloud Computing Forecasts And Market Estimates ,. pages 1–9, 2016.

[70] Randy Conley. Three Levels of Trust - Where Do Your Relationships Stand? 2012.

[71] Claudia Coral and Wolfgang Bokelmann. The role of analytical frameworks for systemic research design, explained in the analysis of drivers and dynamics of historic land-use changes. *Systems*, 5(1):20, 2017.

[72] CPNI. Security for Industrial Control Systems- Manage Third Party Risks. 1:1–16, 2015.

[73] John W Creswell and Vicki L Plano Clark. *Designing and conducting mixed methods research*. Sage publications, 2017.

[74] CSA. Consensus Assessments : Cloud Security Alliance. `https://cloudsecurityalliance.org/group/consensus-assessments/overview`, 2016. (Accessed April 27, 2018).

[75] CSA. Cloud Security Alliance STAR Registry. `https://cloudsecurityalliance.org/star/registry`, 2019. (Accessed March 09, 2019).

[76] Cloud Security Alliance (CSA). Auditing the Cloud Controls Matrix. page 13, 2013.

[77] Norman C Dalkey. The delphi method: An experimental study of group opinion. Technical report, Rand Corp Santa Monica Califonia, 1969.

[78] J. Dana and R. M. Dawes. The Superiority of Simple Alternatives to Regression for Social Science Predictions. *Journal of Educational and Behavioral Statistics*, 29(3):317–331, 2004.

[79] Mohammad Daradkeh, Clare Churcher, and Alan McKinnon. Supporting informed decision-making under uncertainty and risk through interactive visualisation. In *Proceedings of the Fourteenth Australasian User Interface Conference-Volume 139*, pages 23–32. Australian Computer Society, Inc., 2013.

[80] R. Dawes, D Faust, and P. Meehl. Clinical versus actuarial judgment. *Science*, 243(4899):1668–1674, 1989.

[81] Robyn M. Dawes. The robust beauty of improper linear models in decision making. *American Psychologist*, 34(7):571–582, 1979.

[82] Robyn M Dawes and Bernard Corrigan. Linear models in decision making. *Psychological bulletin*, 81(2):95, 1974.

[83] DCMS. Cyber Security Breaches Survey 2018. *Main report - Department for Digital, Culture, Media and Sport*, 2018.

[84] M Dekker and G Hogben. Survey and analysis of security parameters in cloud slas across the european public sector. *ENISA, Tech. Rep.*, 2011.

[85] M. A Dekker. Critical Cloud Computing - A CIIP perspective on cloud computing services. 1(December):33, 2012.

[86] W Edwards Deming. Out of the crisis: Quality. *Productivity and Competitive Position, Massachusetts, USA*, 1986.

[87] Business Dictionary. What is Transparency? definition and meaning. `http://www.businessdictionary.com/definition/transparency.html`, 2018. (Accessed November 05, 2018).

[88] Franz Dietrich, Christian List, A Hájek, and C Hitchcock. Probabilistic opinion pooling. *Oxford Handbook of Philosophy and Probability. Oxford: Oxford University Press. Google Scholar*, 2015.

[89] Karim Djemame, Django J Armstrong, Mariam Kiran, and Ming Jiang. A risk assessment framework and software toolkit for cloud service ecosystems. In *in 2nd International Conference on Cloud Computing, GRIDs, and Virtualization*. Citeseer, 2011.

[90] S. Doborek and Hartmut Werner. *Supply Chain Management*. IGI Global, Jan 2013.

[91] Eileen Doherty, Marian Carcary, and Gerard Conway. Risk Management Considerations in Cloud Computing Adoption. 2012.

[92] Morris R Driels and Young S Shin. Determining the number of iterations for monte carlo simulations of weapon effectiveness. Technical report, Naval Postgraduate School Montery CA Dept of Mechanical and Astronautical, 2004.

[93] Saadia Drissi, Siham Benhadou, and Hicham Medromi. Evaluation of risk assessment methods regarding cloud computing. In *The 5th Conference on Multidisciplinary Design Optimization and Applicaton*, 2016.

[94] Rania El-Gazzar, Eli Hustad, and Dag H. Olsen. Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, 2016.

[95] Kenneth J Ellis, Roman J Shypailo, Dana S Hardin, Maria D Perez, Kathleen J Motil, William W Wong, and Steven A Abrams. Z score prediction model for assessment of bone mineral content in pediatric diseases. *Journal of Bone and Mineral Research*, 16(9):1658–1664, 2001.

[96] Robert J Ellison, John B Goodenough, Charles B Weinstock, and Carol Woody. Evaluating and mitigating software supply chain security risks. Technical report, Carnegie-mellon University, Pittsburgh PA software Eng, Institute, 2010.

[97] ENISA. Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools. (June):177, 2006.

[98] Cohen Eric, Dotson Chris, Edwards Mike, and Gershater Jonathan. Security for Cloud Computing 10 Steps to Ensure Success. *Cloud Standards Customer Council*, pages 1–35, 2015.

[99] Courtney Falk, N Grant St, and W Lafayette. A Model and Tool for Public Cloud Provider Risk Assessment. *Student Paper (Graduate)*, 2014.

[100] Kaniz Fatema, Vincent C. Emeakaroha, Philip D. Healy, John P. Morrison, and Theo Lynn. A survey of Cloud monitoring tools: Taxonomy, capabilities and objectives. *Journal of Parallel and Distributed Computing*, 74(10):2918–2933, 2014.

[101] Massimo Felici and Siani Pearson. Accountability for data governance in the cloud. In Massimo Felici and Carmen Fernández-Gago, editors, *Lecture Notes in Computer Science*, volume 8937, chapter Accountability, pages 3–42. Springer International Publishing, 2015.

[102] José Luis Fernández-Alemán, Inmaculada Carrión Señor, Pedro Ángel Oliver Lozoya, and Ambrosio Toval. Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3):541–562, 2013.

[103] Finantisvalue. How to estimate the value of your software or digital products? - Finantis Value. `http://www.finantisvalue.com/en/how-to-estimate-the-value-of-your-software-or-digital-products/`, 2018. (Accessed March 05, 2019).

[104] Simone Fischer-Hübner, Julio Angulo, and Tobias Pulls. How can cloud users be supported in deciding on, tracking and controlling how their data are used? In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pages 77–92. Springer, 2013.

[105] J Oriol Fitó, Mario Macías, and Jordi Guitart. Toward business-driven risk management for cloud computing. In *2010 International Conference on Network and Service Management*, pages 238–241. IEEE, 2010.

[106] Jane Forman and Laura Damschroder. Qualitative content analysis. In *Empirical methods for bioethics: A primer*, pages 39–62. Emerald Group Publishing Limited, 2007.

[107] Jay W Forrester. Industrial dynamicsafter the first decade. *Management Science*, 14(7):398–415, 1968.

[108] Jay W Forrester. System dynamics and the lessons of 35 years. In *A systems-based approach to policymaking*, pages 199–240. Springer, 1993.

[109] Jay W Forrester. System dynamics, systems thinking, and soft or. *System dynamics review*, 10(2-3):245–256, 1994.

[110] Jay Wright Forrester. *Market growth as influenced by capital investment*. Industrial Management Review, 1968.

[111] Frank Fowley and Claus Pahl. Cloud migration architecture and pricing - Mapping a licensing business model for software vendors to a SaaS business model. *Commun. Comput. Inf. Sci.*, 707(September):91–103, 2018.

[112] Jack Freund and Jack Jones. *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann, 2014.

[113] Sailesh Gadia. Cloud Computing Risk Assessment: A Case Study. *ISACA journal*, 4:11–16, 2011.

[114] R Gaonkar and N Viswanadham. A conceptual and analytical framework for the management of risk in supply chains. *Robotics and Automation, 2004. Proceedings. ICRA '04. 2004 IEEE International Conference on*, 3(April):2699–2704 Vol.3, 2004.

[115] Elizabeth Garnsey and James McGlade. *Complexity and co-evolution: continuity and change in socio-economic systems*. Edward Elgar Publishing, 2006.

[116] Abhijeet Ghadge, Samir Dani, Michael Chester, and Roy Kalawsky. A systems approach for modelling supply chain risks. *Supply chain management: an international journal*, 18(5):523–538, 2013.

[117] Vahid Ghafori and Reza Manouchehri Sarhadi. Best Cloud Provider Selection using Integrated ANP-DEMATEL and Prioritizing SMI Attributes. *International Journal of Computer Applications*, 71(16):18–25, 2013.

[118] Martin Gill, Emmeline Taylor, Tom Bourne, and Gemma Keats. Organisational perspectives on the value of security. *Security Research Initiative (SRI) report*, 2008.

[119] Jeffrey Goldstein. Emergence as a construct: History and issues. *Emergence*, 1(1):49–72, 1999.

[120] Theodore Gordon and Adam Pease. Rt delphi: An efficient,round-less, almost real time delphi method. *Technological Forecasting and Social Change*, 73(4):321–333, 2006.

[121] Lazaros Goutas, Juliana Sutanto, and Hassan Aldarbesti. The building blocks of a cloud strategy: evidence from three SaaS providers. *Communications of the ACM*, 59(1):90–97, 2015.

[122] Mark Graban. Measures of Success: React Less, Lead Better, Improve More, 2018.

[123] Donna Gresh, Lea a. Deleris, and Luca Gasparini. Visualizing Risk. *Proc. IEEE Symp. Inf. Vis.*, 25293, 2011.

[124] The Open Group. Technical Standard Risk Taxonomy. `http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf`, 2009. (Accessed January 13, 2019).

[125] Katarzyna Grzybowska, Gábor Kovács, and Balázs Lénárt. The supply chain in cloud computing. *Research in Logistics & Production*, 4(1):33–44, 2014.

[126] Jan Gulliksen, Bengt Göransson, Inger Boivie, Stefan Blomkvist, Jenny Persson, and Åsa Cajander. Key principles for user-centred systems design. *Behaviour and Information Technology*, 22(6):397–409, 2003.

[127] Talal Halabi and Martine Bellaiche. Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications*, 33:55–65, 2017.

[128] Ralph Hall. Mixed methods: In search of a paradigm. *Vortrag. Download (am 10.01. 2013) under: http://www. auamii. com/proceedings_Phuket_2012/Hall. pdf*, 2012.

[129] Hans Krause Hansen. Numerical operations, transparency illusions and the datafication of governance. *European Journal of Social Theory*, 18(2):203–220, 2015.

[130] Qusay F. Hassan, Alaa M. Riad, and Ahmed E. Hassan. Understanding Cloud Computing. *Software Reuse in the Emerging Cloud Computing Era*, (April):204–227, 2011.

[131] Reid Hastie. Problems for judgment and decision making. *Annual review of psychology*, 52(1):653–683, 2001.

[132] Nick Hayes and Trevor Lyness. The Forrester New Wave: Cybersecurity Risk Rating Solutions, Q4 2018. `https://www.forrester.com/report/The+Forrester+New+Wave+Cybersecurity+Risk+Rating+Solutions+Q4+2018/-/E-RES142874{#}`, 2018. (Accessed November 15, 2018).

[133] Rick Hefner. Lessons learned with the systems security engineering capability maturity model. *Proceedings of the 19th international conference on Software engineering - ICSE '97*, 35:566–567, 1997.

[134] Max Henrion. Propagating uncertainty in bayesian networks by probabilistic logic sampling. In *Machine Intelligence and Pattern Recognition*, volume 5, pages 149–163. Elsevier, 1988.

[135] Raoul Hentschel, Christian Leyh, and Anne Petznick. Current cloud challenges in germany: the perspective of cloud service providers. *Journal of Cloud Computing*, 7(1):5, 2018.

[136] Harry Hermanns. Interviewing as an activity. *A companion to qualitative research*, 1, 2004.

[137] Heron Julia. Supply Chain Security-Tick box compliance no longer enough. `https://www.isms.online/general-data-protection-regulation-gdpr/supply-chain-security-tick-box-compliance-no-longer-enough/`, 2018. (Accessed July 07, 2019).

[138] Richard Hibbert. Extended Enterprise : Managing risk in complex. *Institute of Risk Managament*, 2014.

[139] Scott Hilton. Dyn Analysis Summary Of Friday October 21 Attack — Dyn Blog. `https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/`, 2016. (Accessed March 31, 2017).

[140] Rick Hogan. Introduction to Statistics for Uncertainty Analysis. `http://www.isobudgets.com/introduction-statistics-uncertainty-analysis/`, 2016. (Accessed September 26, 2018).

[141] Chia-Chien Hsu and Brian A. Sandford. The Delphi Technique : Making Sense Of Consensus. *Pract. Assessment, Res. Eval.*, 12(10):1–8, 2007.

[142] Douglas W. Hubbard. *Book Review The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons, 2010.

[143] Douglas W. Hubbard and Richard Seiersen. Risk Matrices, Lie Factors, Misconceptions, and Other Obstacles to Measuring risk. In *How to Measure Anything in Cybersecurity Risk*. 2016.

[144] Investopedia. Z-Score. `http://www.investopedia.com/terms/z/zscore.asp`, 2017. (Accessed May 01, 2017).

[145] Dan Ionita. Current established risk assessment methodologies and tools. Master's thesis, University of Twente, 2013.

[146] Dan Ionita. *Model-Driven Information Security Risk Assessment of Socio-Technical Systems*. PhD thesis, 2018.

[147] ISACA. *COBIT: A Business Framework for the Governance and Management of Enterprise IT*. 2013.

[148] ISACA & CSA. Cloud Computing Market Maturity. *AN ISACA CLOUD Vis. Ser. WHITE Pap.*, pages 1–12, 2015.

[149] Shareeful Islam, Stefan Fenz, Edgar Weippl, and Haralambos Mouratidis. A Risk Management Framework for Cloud Migration Decision Support. *J. Risk Financ. Manag.*, 10(2):10, 2017.

[150] Umar Mukhtar Ismail, Shareeful Islam, Moussa Ouedraogo, and Edgar Weippl. A framework for security transparency in Cloud Computing. *Future Internet*, 8(1), 2016.

[151] International Standards Organisation (ISO). ISO 27005:2011. *Information technology. Security techniques. Information security risk management*, 2011.

[152] ISO31000-2009. ISO31000:2009 - Risk management: Principles and guidleines, 2009.

[153] ISO/IEC. ISO/IEC 27001:2013: Information technology Security techniques Information security management systems Requirements, 2013.

[154] Yashpalsinh Jadeja and Kirit Modi. Cloud computing - Concepts, architecture and challenges. *2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012*, pages 877–880, 2012.

[155] Pooyan Jamshidi, Aakash Ahmad, and Claus Pahl. Cloud migration research: a systematic review. *IEEE Transactions on Cloud Computing*, 1(2):142–157, 2013.

[156] Wayne Jansen and Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication 800*, 144(7):1–70, 2011.

[157] Maria Jenks. Critical Infrastructure Protection Supply Chain Risk Management. pages 1–6, 2016.

[158] Jisc. Attitudes to Risk. *Risk Managamen Guide*, (November), 2012.

[159] C . W Johnson. You Outsource the Service but Not the Risk : Supply Chain Risk Management for the Cyber Security of Safety Critical Systems . In : 34th International System Safety Conference , Orlanda , FL , USA , 8-12. (November):8–12, 2016.

[160] R Burke Johnson and Anthony J Onwuegbuzie. Mixed methods research: A research paradigm whose time has come. *Educational researcher*, 33(7):14–26, 2004.

[161] Jonathan Greer. Taking a Chance with Monte Carlo. `https://www.panaseer.com/2015/09/30/taking-a-chance-with-monte-carlo/`, 2015. (Accessed March 20, 2017).

[162] Jack A. Jones. An Introduction to Factor Analysis of Information Risk. *Risk Management Insight*, 2005.

[163] Bineet Kumar Joshi, Mohit Kumar Shrivastava, and Bansidhar Joshi. Security threats and their mitigation in infrastructure as a service. *Perspectives in Science*, 8:462–464, 2016.

[164] Daniel Kahneman, Paul Slovic, and Amos Tversky. *Judgment under uncertainty: Heuristics and biases*. Cambridge university press, 1982.

[165] Burton S Kaliski Jr and Wayne Pauley. Toward risk assessment as a service in cloud environments. *Proc. 2nd USENIX Conf. Hot Top. cloud Computing*, 10(10):1–7, 2010.

[166] Muhammad Mustafa Kamal. Investigating Enterprise Application Integration Adoption in the Local Government Authorities. In *Handbook of Research on Strategies for Local E-Government Adoption and Implementation: Comparative Studies*, volume 2, pages 661–686. Brunel University, School of Information Systems, Computing and Mathematics, 2009.

[167] Bilge Karabacak and Ibrahim Sogukpinar. ISRAM: Information security risk analysis method. *Computers and Security*, 24(2):147–159, 2005.

[168] Michael J. Kavis. *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. 2014.

[169] Ali Khajeh-Hosseini, Ian Sommerville, Jurgen Bogaerts, and Pradeep Teregowda. Decision support tools for cloud migration in the enterprise. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pages 541–548. IEEE, 2011.

[170] Afnan Ullah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, and Karim Djemame. Security risks and their management in cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 121–128. IEEE, 2012.

[171] Anastasia Kholod. APIs for SaaS Vendors: Why A Vital Need? `https://www.api2cart.com/blog/apis-saas-vendors-vital-need/`, 2016. (Accessed January 12, 2019).

[172] Frank H Knight. *Risk, uncertainty and profit*. Courier Corporation, 2012.

[173] Ryan Ko, Stephen Lee, and V Rajan. Cloud Computing Vulnerability Incidents: A Statistical Overview. *Cloud Security Alliance*, page 21, 2013.

[174] Ryan K.L. Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, and Bu Sung Lee. TrustCloud: A framework for accountability and trust in cloud computing. *Proceedings - 2011 IEEE World Congress on Services, SERVICES 2011*, pages 584–588, 2011.

[175] Will Koehrsen. The Poisson Distribution and Poisson Process Explained. `https://towardsdatascience.com/the-poisson-distribution-and-poisson-process-explained-4e2cb17d459`, 2019. (Accessed July 18, 2019).

[176] E Kreyszig. *Advanced Engineering Mathematics. Fourth edi.* John Wiley & Sons, Inc, 1979.

[177] Paul Krill. The risks and rewards of the age of APIs. `http://www.infoworld.com/article/2609135/apis/development-tools-the-risks-and-rewards-of-the-age-of-apis.html`, 2013. (Accessed November 17, 2018).

[178] Kenji E. Kushida, Jonathan Murray, and John Zysman. Cloud Computing: From Scarcity to Abundance. *Journal of Industry, Competition and Trade*, 15(1):5–19, 2015.

[179] Kenji E. Kushida, Jonathan Murray, and John Zysman. Cloud Computing: From Scarcity to Abundance. *Journal of Industry, Competition and Trade*, 15(1):5–19, 2015.

[180] Michael Lang, Manuel Wiesche, and Helmut Krcmar. Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes. *Information and Management*, 2018.

[181] Jens Lansing and Ali Sunyaev. Trust in Cloud Computing. *ACM SIGMIS Database*, 47(2):58–96, 2016.

[182] Michael D Larsen. The Psychology of Survey Response. *Journal of the American Statistical Association*, 97(457):358–359, 2002.

[183] Stefanie Leimeister, Christoph Riedl, Markus Böhm, and Helmut Krcmar. The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks. *Proceedings of 18th European Conference on Information Systems ECIS 2010*, (Ecis 2010):1–12, 2010.

[184] Riyana Lewis, Panos Louvieris, and Pamela Abbott. Cybersecurity Information Sharing : a Framework for Information Security. *Twenty Second European Conference on Information Systems*, pages 1–15, 2014.

[185] Ang Li, Xiaowei Yang, Srikanth Kandula, and Ming Zhang. CloudCmp: Comparing Public Cloud Providers. *Proceedings of the 10th annual conference on Internet measurement - IMC '10*, 15(2):1, 2010.

[186] Feng Li, Jun-qi Hou, and Dao-ming Xu. Managing disruption risks in supply chain. In *2010 IEEE International Conference on Emergency Management and Management Sciences*, pages 434–438. IEEE, 2010.

[187] Yvonna S Lincoln and Egon G Guba. *Naturalistic Inquiry*. SAGE Publications: Newbury Park, CA, 1985.

[188] Maik Lindner, Clovis Chapman, Stuart Clayman, Daniel Henriksson, and Erik Elmorth. The Cloud Supply Chain : A Framework for Information , Monitoring , Accounting and Billing. *2nd International ICST Conference on Cloud Computing*, 2010.

[189] Harold A Linstone, Murray Turoff, et al. *The delphi method*. Addison-Wesley Reading, MA, 1975.

[190] Peiyu Liu and Dong Liu. The new risk assessment model for information system in Cloud Computing Environment. *Procedia Engineering*, 15:3200–3204, 2011.

[191] Nate Lord. Data Security Experts Reveal the Biggest Mistakes Companies Make with Data & Information Security — Digital Guardian, 2016.

[192] Nikolaos Loutas, Eleni Kamateri, Filippo Bosi, and Konstantinos Tarabanis. Cloud computing interoperability: The state of play. *Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011*, pages 752–757, 2011.

[193] Lumina Decision Systems. Check attribute - Analytica Wiki. `https://wiki.analytica.com/index.php?title=Check_attribute`. (Accessed March 27, 2019).

[194] Jesus Luna, Neeraj Suri, Michaela Iorga, and Anil Karmel. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards. *IEEE Cloud Computing*, 2(3):32–40, 2015.

[195] Matt Makai. Introduction to Flask. `https://www.fullstackpython.com/flask.html`, 2019. (Accessed May 18, 2019).

[196] Louis Marinos. ENISA threat taxonomy: A tool for structuring threat information. Initial report. *ENISA*, (January):1–24, 2016.

[197] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, and Anand Ghalsasi. Cloud computing - The business perspective. *Decision Support Systems*, 51(1):176–189, 2011.

[198] Loretta Maxfield. Managing commercial risk within the supply chain post - GDPR.Report. `https://gdpr.report/news/2018/08/31/managing-commercial-risk-within-the-supply-chain-post/`, 2018. (Accessed February 27, 2019).

[199] Mike Mcfarland. Best Practices in Cyber Supply Chain Risk Management. *NIST*, pages 1–3, 2015.

[200] Hugh P McKenna. The delphi technique: a worthwhile research approach for nursing? *Journal of advanced nursing*, 19(6):1221–1225, 1994.

[201] Charles McLellan. Saas Pros Cons and Leading Vendors. `https://www.zdnet.com/article/saas-pros-cons-and-leading-vendors/` , 2013. (Accessed October 27, 2018).

[202] Microsoft. The Security Risk Management Guide. *Microsoft Solutions for Security and Compliance*, 35-72, 2006.

[203] Microsoft. Trusted Cloud : Microsoft Azure Security, Privacy, and Compliance. *Microsoft Corporation*, (April):20, 2015.

[204] Scott B Miles. Participatory model assessment of earthquake-induced landslide hazard models. *Natural hazards*, 56(3):749–766, 2011.

[205] John H Miller and Scott E Page. *Complex adaptive systems: An introduction to computational models of social life*, volume 17. Princeton university press, 2009.

[206] Minitab. A Comparison of the Pearson and Spearman Correlation Methods. `https://support.minitab.com/en-us/minitab-express/1/help-and-how-to/modeling-statistics/regression/supporting-topics/basics/a-comparison-of-the-pearson-and-spearman-correlation-methods/`, 2014. (Accessed February 02, 2019).

[207] David L Morgan. Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of mixed methods research*, 1(1):48–76, 2007.

[208] Timothy Morrow and Donald Faatz. 12 Risks, Threats, and Vulnerabilities in Moving to the Cloud. `https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html`, 2018. (Accessed March 13, 2019).

[209] Gianmario Motta, Linlin You, Nicola Sfondrini, Daniele Sacco, and Tianyi Ma. Service level management (slm) in cloud computing third party slm framework. In *2014 IEEE 23rd International WETICE Conference*, pages 353–358. IEEE, 2014.

[210] Laura Muñiz-Rodríguez, Pedro Alonso, Luis J. Rodríguez-Muñiz, and Martin Valcke. Developing and validating a competence framework for secondary mathematics student teachers through a Delphi method. *J. Educ. Teach.*, 43(4):383–399, 2017.

[211] Michael D. Myers and Michael Newman. The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1):2–26, 2007.

[212] Sang Ho Na and Eui Nam Huh. A methodology of assessing security risk of cloud computing in user perspective for security-service-level agreements. *4th International Conference on Innovative Computing Technology, INTECH 2014 and 3rd International Conference on Future Generation Communication Technologies, FGCT 2014*, pages 87–92, 2014.

[213] National Cyber Security Centre (NCSC). Understanding supply chain risk, 2018.

[214] Neo4j. The Neo4j Graph Platform. The #1 Platform for Connected Data. `https://neo4j.com/`, 2016. (Accessed September 19, 2018).

[215] Steve New. Supply chain traceability and product provenance: Challenges for theory and practice. In *Supply Chain Management and Logistics in a Volatile Global Environment*. Blackhall Publishing, Dublin, 2009.

[216] Steve New and Dana Brown. The Four Challenges of Supply Chain Transparency. *European Business Review*, pages 1–7, 2012.

[217] Steve New and Roy Westbrook. *Understanding supply chains: concepts, critiques, and futures*. OUP Oxford, 2004.

[218] Lee Newcombe. *Securing cloud services: a pragmatic approach to security architecture in the cloud*. IT Governance Publishing, 2012.

[219] Shaun Nichols. AWS's S3 outage was so bad Amazon couldn't get into its own dashboard to warn the world. `https://www.theregister.co.uk/2017/03/01/aws_s3_outage/`, 2017. (Accessed May 22, 2017).

[220] NIST. Standards for security categorization of federal information and information systems. Technical report, National Institute of Standards and Technology, Gaithersburg, MD, 2004.

[221] NIST. Security and privacy controls for federal information systems and organizations. *NIST Special Publication 800-53*, (800-53 revision 4), 2015.

[222] Yudhistira Nugraha, Ian Brown, and Ashwin Sasongko Sastrosubroto. An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements. *IEEE Transactions on Emerging Topics in Computing*, 2016.

[223] Jason R C Nurse, Sadie Creese, and David De Roure. Security risk assessment in internet of things systems. *IEEE IT Professional*, 19(5):20–26, 2017.

[224] Jason R C Nurse, Petar Radanliev, Sadie Creese, and David De Roure. If you can't understand it, you can't properly assess it! the reality of assessing security risks in internet of things systems. In *Living in the Internet of Things: Cybersecurity of the IoT-2018*, pages 1–9. IET, 2018.

[225] Federation of Small Business (FSB). Chain Reaction: Improving the Supply Chain Experience for Smaller Firms. 2018.

[226] Chitu Okoli and Suanne D. Pawlowski. The Delphi method as a research tool: An example, design considerations and applications. *Information and Management*, 42(1):15–29, 2004.

[227] Jacob Olcott. Input to the Commission on Enhancing National Cybersecurity: The Impact of Security Ratings on National Cybersecurity, 2016.

[228] Luis Olsina and Gustavo Rossi. Measuring web application quality with webqem. *IEEE Multimedia*, 9(4):20–29, 2002.

[229] Olusola Akinrolabu. Survey - Supply Chain Cyber Risks in Cloud Computing: The Effect of Transparency on Risk Assessment. https://oxford.onlinesurveys.ac.uk/supply-chain-cyber-risks-in-cloud-computing-the-effect, 2017.

[230] Ugochukwu Onwudebelu and Benedict Chukuka. Will adoption of cloud computing put the enterprise at risk? *Proceedings of the 2012 IEEE 4th International Conference on Adaptive Science and Technology, ICAST 2012*, pages 82–85, 2012.

[231] Python Org. Python For Beginners. https://www.python.org/about/gettingstarted/, 2019. (Accessed April 19, 2019).

[232] Emma Osborn and Andrew Simpson. On small-scale IT users' system architectures and cyber security: A UK case study. *Comput. Secur.*, 70:27–50, 2017.

[233] OWASP. OWASP Top Ten Project. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, 2018. (Accessed January 02, 2019).

[234] Palisade. Monte Carlo Simulation: What Is It and How Does It Work? http://www.palisade.com/risk/monte_carlo_simulation.asp, 2017. (Accessed May 02, 2017).

[235] Palisade. @RISK: Risk Analysis using Monte Carlo Simulation in Excel and Project. http://www.palisade.com/risk/monte_carlo_simulation.asp, 2018. (Accessed October 19, 2018).

[236] David J Pannell. Sensitivity analysis: strategies, methods, concepts, examples. *Agric Econ*, 16:139–152, 1997.

[237] Alain Pannetrat and Jesus Luna. Standards for accountability in the cloud. In Massimo Felici and Carmen Fernández-Gago, editors, *Lecture Notes in Computer Science*, volume 8937, pages 275–288. Springer International Publishing, 2015.

[238] Fawaz Paraiso, Nicolas Haderer, Philippe Merle, Romain Rouvoy, and Lionel Seinturier. A federated multi-cloud PaaS infrastructure. *Proceedings - 2012 IEEE 5th International Conference on Cloud Computing, CLOUD 2012*, pages 392–399, 2012.

[239] Geet Parekh, David Delatte, Geoffrey L. Herman, Linda Oliva, Dhananjay Phatak, Travis Scheponik, and Alan T. Sharman. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education*, 2018.

[240] Paul Venezia. Murder in the Amazon cloud - The demise of Code Spaces at the hands of an attacker. *InfoWorld*, pages 1–4, 2016.

[241] Siani Pearson. Towards Accountability in cloud.pdf. *HP Labs Tech.Report*, 15(4):64–69, 2011.

[242] Siani Pearson. Data Protection in the Cloud. *Cloud Security Alliance Online*, 1:10–13, 2016.

[243] Siani Pearson, Vasilis Tountopoulos, Daniele Catteddu, Mario Sudholt, Refik Molva, Christoph Reich, Simone Fischer-Hubner, Christopher Millard, Volkmar Lotz, Martin Gilje Jaatun, Ronald Leenes, Chunming Rong, and Javier Lopez. Accountability for cloud and other future Internet services. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, 3:629–632, 2012.

[244] Anderson Philip. Complexity theory and organization science. *Organization science*, 10(3):216–232, 1999.

[245] Power. The risk management of everything. *J. Risk Financ.*, 5(3):58–65, 2004.

[246] Michael Power. *Organized Uncertainty - Designing a world of risk management*. Oxford University Press, 2007.

[247] Ling Qian, Zhiguo Luo, Yujian Du, and Leitao Guo. Cloud computing: An overview. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 5931 LNCS, pages 626–631, 2009.

[248] Raj Samani. Common Assurance Maturity Model. pages 1–2, 2011.

[249] Norman C Rasmussen. The application of probabilistic risk assessment techniques to energy technologies. *Annual Review of Energy*, 6(1):123–138, 1981.

[250] Mary Kay Rayens and Ellen J. Hahn. Building Consensus Using the Policy Delphi Method. *Policy, Politics, & Nursing Practice*, 1(4):308–315, 2000.

[251] General Data Protection Reg. EU Approves GDPR. *Inf. Manag. J.*, 50(4):7, 2016.

[252] Jonas Repschläger, Stefan Wind, Rüdiger Zarnekow, and Klaus Turowski. Developing a cloud provider selection model. In *EMISA*, pages 163–176, 2011.

[253] Barry Ribbeck. Cloud Service Provider Risk Assessment. `https://events.educause.edu/annual-conference/2014/proceedings/cloud-service-provider-risk-assessment`, 2014. (Accessed August 20, 2018).

[254] Judy Robertson. Likert-type scales, statistical methods, and effect sizes. *Communications of the ACM*, 55(5):6–7, 2012.

[255] Ian Robinson, Jim Webber, and Emil Eifrem. *Graph databases: new opportunities for connected data*. " O'Reilly Media, Inc.", 2015.

[256] Chunming Rong, Son T. Nguyen, and Martin Gilje Jaatun. Beyond lightning: A survey on security challenges in cloud computing. *Computers and Electrical Engineering*, 39(1):47–54, 2013.

[257] Ronald S Ross. Managing information security risk: Organization, mission, and information system view. Technical report, 2011.

[258] Ronald S Ross. Guide for conducting risk assessments. *Special Publication (NIST SP) - 800-30 Rev 1*, 1(September):95, 2012.

[259] Artur Rot. IT Risk Assessment : Quantitative and Qualitative Approach. *Proceedings of The World Congress on Engineering and Computer Science 2008*, pages 1073–1078, 2008.

[260] Edward Royce. H.R.5793 - 113th Congress (2013-2014): Cyber Supply Chain Management and Transparency Act of 2014. 2014.

[261] Keyun Ruan. Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, 65:77–89, 2017.

[262] Nayan B Ruparelia and Nayan Ruparelia. *Cloud computing*. MIT Press, 2016.

[263] Mehmet Sahinoglu and Scott Morton. Cloud risk-o-meter: An algorithm for cloud risk assessment and management. In *Conference of Society of Design and Process Science (SDPS), Session X1 Cloud Computing: Security and Reliability*, volume 1, pages 30–3, 2012.

[264] Mari Sako. *Price, quality and trust: Inter-firm relations in Britain and Japan*. Number 18. Cambridge University Press, 1992.

[265] Dina Salah, Richard Paige, and Paul Cairns. An evaluation template for expert review of maturity models. In *International Conference on Product-Focused Software Process Improvement*, pages 318–321. Springer, 2014.

[266] Andrea Saltelli, Marco Ratto, Terry Andres, Francesca Campolongo, Jessica Cariboni, Debora Gatelli, Michaela Saisana, and Stefano Tarantola. *Global sensitivity analysis: the primer*. John Wiley & Sons, 2008.

[267] Raj Samani, Brian Honan, and Jim Reavis. *CSA Guide to Cloud Computing*. Number 1. 2015.

[268] Kristopher Sandoval. Your API is Vulnerable: 4 Risks to Mitigate — Nordic APIs, 2015.

[269] SANS. SANS Auditing Networks — Perimeter IT Audit — IT Systems Audit, 2019.

[270] SANS Institute. SANS Institute - Critical Security Controls. `https://www.sans.org/critical-security-controls/`, 2016. (Accessed September 17, 2018).

[271] Prasad Saripalli and Ben Walters. Quirc: A quantitative impact and risk assessment framework for cloud security. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pages 280–288. IEEE, 2010.

[272] Mark Saunders, Philip Lewis, and Adrian Thornhill. *Research methods for business students*. Pearson education, 2009.

[273] Roy C Schmidt. Managing delphi surveys using nonparametric statistical techniques. *decision Sciences*, 28(3):763–774, 1997.

[274] Ron Schmitting. Performing a Security Risk Assessment. *ISACA Journal*, 1, 2010.

[275] Bruce Schneier. Should Companies Do Most of Their Computing in the Cloud? (Part 1) - Schneier on Security, 2015.

[276] Ing Jürgen Schwarz and Ing Pedro Maria Sánchez. *Implementation of Artificial Intelligence into Risk Management Decision-making processes in Construction projects*. Universität der Bundeswehr München, Institut für Baubetrieb, 2015.

[277] Nevin S Scrimshaw and Gary R Gleason. *Rapid assessment procedures: qualitative methodologies for planning and evaluation of health related programmes*. International Nutrition Foundation for Developing Countries Boston, 1992.

[278] Alireza Shameli Sendi and Mohamed Cheriet. Cloud computing: A risk assessment model. In *Cloud Engineering (IC2E), 2014 IEEE International Conference on*, pages 147–152. IEEE, 2014.

[279] Mahesh U. Shankarwar and Ambika V. Pawar. Security and privacy in cloud computing: A survey. *Advances in Intelligent Systems and Computing*, 328:1–11, 2015.

[280] Shared Assessments. Evaluating Cloud Risk for the Enterprise : A Shared Assessments Guide. (October):53, 2010.

[281] Yossi Sheffi and James B Rice Jr. A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review*, 47(1):41–48, 2005.

[282] Mark Sherman. Risks in the Software Supply Chain. *Software Solutions Symposium*, pages 1–36, 2017.

[283] Grant Shirk. Ask Suppliers These 8 Questions to Measure GDPR Compliance. `https://www.scoutrfp.com/2018/04/sourcing-gdpr-compliance-questions-suppliers/`, 2018. (Accessed February 12, 2019).

[284] Kristin S Shrader-Frechette. Perceived risks versus actual risks: Managing hazards through negotiation. *Risk*, 1:341, 1990.

[285] Jane Siegel and Jeff Perdue. Cloud services measures for global use: the service measurement index (smi). In *SRII Global Conference (SRII), 2012 Annual*, pages 411–415. IEEE, 2012.

[286] K. Sigler, D. Shoemaker, and A. Kohnke. *Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product*. Internal Audit and IT Audit. Auerbach, 2017.

[287] H Simon. The Sciences of the Artificial 3rd edition MIT Press. *Cambridge, MA*, 1996.

[288] Herbert A Simon. The architecture of complexity. *Proceedings of the American Philosophical Society*, 106(6):467–482, 1962.

[289] Yogeshwaran Sivasubramanian, Syed Zubair Ahmed, and Ved Prakash Mishra. Risk Assessment for Cloud Computing. *International Research Journal of Electronics and Computer Engineering*, 3(2):7, 2017.

[290] Paul Slovic. Perceived risk, trust, and democracy. *Risk analysis*, 13(6):675–682, 1993.

[291] B. Snaith, M. Hardy, and Alison Walker. Emergency ultrasound in the prehospital setting: The impact of environment on examination outcomes. *Emergency Medicine Journal*, 28(12):1063–1065, 2011.

[292] Ian Sommerville. *Software engineering 9th Edition*. Addison-wesley, 2011.

[293] SourceMap. End-to-End Supply Chain Visualization. `https://www.sourcemap.com/blog/end-to-end-supply-chain-visualization-white-paper`, 2016. (Accessed March 02, 2019).

[294] Susan K Soy. The case study as a research method: Uses and users of information. *School of information*, 1997.

[295] Alice Squires, Jon Wade, Pete Dominick, and Don Gelosh. Building a competency taxonomy to guide experience acceleration of lead program systems engineers. Technical report, Stevens Institute of Tech Hoboken NJ School of Systems and Enterprises, 2011.

[296] SSAE 16. SOC 2 Report Trust Services Principles — The SSAE 16 Reporting Standard. 2015.

[297] John Sterman. System dynamics: systems thinking and modeling for a complex world. 2002.

[298] Sytse Strijbos. *Systems thinking*. Oxford University: Oxford, 2010.

[299] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11, 2011.

[300] Sinje Sung and Sangmok Kang. The trust levels, trust determinants, and spatial dimensions in inter-firm relationships: A warehousing firms perspective in the city of busan, south korea. *iBusiness*, 4(04):371, 2012.

[301] Linda Booth Sweeney and John D Sterman. Bathtub dynamics: initial results of a systems thinking inventory. *System Dynamics Review*, 16(4):249–286, 2000.

[302] Nassim Nicholas Taleb and Mark Blyth. The black swan of cairo: How suppressing volatility makes the world less predictable and more dangerous. *Foreign Affairs*, pages 33–39, 2011.

[303] Srinivas Talluri, Ram Narasimhan, and Anand Nair. Vendor performance with supply risk: A chance-constrained DEA approach. *International Journal of Production Economics*, 100(2):212–222, 2006.

[304] Changlong Tang and Jiqiang Liu. Selecting a trusted cloud service provider for your SaaS program. *Computers and Security*, 50:60–73, 2015.

[305] Hua Tang, Jiejun Yang, Xiaofang Wang, and Qi Zhou. A Research for Cloud Computing Security Risk Assessment. *The Open Cybernetics & Systemics Journal*, 10(1):210–217, 2016.

[306] Charles Teddlie and Abbas Tashakkori. *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences*. Sage, 2009.

[307] Telegraph. How a fat-finger typo took down the internet earlier this week (according to Amazon). http://www.telegraph.co.uk/technology/2017/03/03/amazon-blames-fat-finger-typo-taking-huge-chunk-internet/, 2017. (Accessed May 22, 2017).

[308] Tenable Network Security. 2017 Global Cybersecurity Assurance Report Card. 1:19, 2017.

[309] Marianthi Theoharidou, Nikolaos Tsalis, and Dimitris Gritzalis. In Cloud We Trust: Risk-Assessment-as-a-Service. *Trust Management VII*, 401:100–110, 2013.

[310] S Thiebes, D Scheidt, M Schmidt-Kraepelin, Alexander Benlian, Ali Sunyaev, et al. Paving the way for real-time delphi in information systems research: A synthesis of survey instrument designs and feedback mechanisms. Technical report, Darmstadt Technical University, Department of Business Administration, Economics and Law, Institute for Business Studies (BWL), 2018.

[311] Clif Triplett. Security is Only as Strong as the Weakest Link - Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/strong-weakest-link/, 2019. (Accessed December 23, 2019).

[312] Barbara Tversky and Paul U Lee. Pictorial and verbal tools for conveying routes. In *International Conference on Spatial Information Theory*, pages 51–64. Springer, 1999.

[313] Samuel Tweneboah-Koduah and William J Buchanan. Security risk assessment of critical infrastructure systems: A comparative study. *The Computer Journal*, 61(9):1389–1406, 2018.

[314] Upguard. Why Should I Care About Cyber Risk? https://www.upguard.com/blog/why-should-i-care-about-cyber-risk, 2018. (Accessed April 25, 2018).

[315] John Urry. The complexity turn. *Theory, culture & society*, 22(5):1–14, 2005.

[316] USA Department of Homeland Security and USA Department of Energy. Cybersecurity Capability Maturity Model (C2M2) (white paper). *Department of Homeland Security*, (February), 2014.

[317] Chiara Verbano and Karen Venturini. Managing Risks in SMEs: A Literature Review and Research Agenda. *Journal of technology management & innovation*, 8(3):33–34, 2013.

[318] Vilhelm Verendel. Quantified security is a weak hypothesis. *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*, page 37, 2009.

[319] S VivinSandar and Sudhir Shenai. Economic denial of sustainability (edos) in cloud services using http and xml based ddos attacks. *International Journal of Computer Applications*, 41:11–16, 03 2012.

[320] David Vohradsky. Cloud Risk – 10 Principles and a Framework for Assessment. *ISACA Journal*, 5:31–41, 2012.

[321] R Hevner Von Alan, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, 28(1):75–105, 2004.

[322] Ludwig Von Bertalanffy. General system theory. *New York*, 41973(1968):40, 1968.

[323] David Vose. *Risk analysis: a quantitative guide*. John Wiley & Sons, 2008.

[324] Gaute Wangen, Christoffer Hallstensen, and Einar Snekkenes. A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17(6):681–699, 2018.

[325] Rolf H Weber and Dominic Nicolaj Staiger. Cloud Computing: A cluster of complex liability issues. *Web Journal of Current Legal Issues; Vol 20, No 1 (2014): Web JCLI*, 20(1):1–13, 2014.

[326] Aaron Weiss. Computing in the clouds. *NetWorker*, 11(4):16–25, 2007.

[327] Lisa Van Der Werff, Theo Lynn, and HH Xiaong. Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label, 2014.

[328] Andreas Wieland and Carl Marcus Wallenburg. Dealing with supply chain risks. *International Journal of Physical Distribution & Logistics Management*, 42(10):887–905, 2012.

[329] Bill Williams. The Economics of Cloud Computing: An Overview For Decision Makers. *Cisco Press*, pages 5–20, 2012.

[330] J.D. Wisner, K.C. Tan, and G.K. Leong. *Principles of supply chain management: A balanced approach*, volume 43. 2016.

[331] R.K. Yin. *Case Study Research: Design and Methods*. SAGE Publications, 2013.

[332] Lamia Youseff, Maria Butrico, and Dilma Da Silva. Toward a unified ontology of cloud computing. In *Grid Computing Environments Workshop, GCE 2008*, 2008.

[333] Yung Chou. Cloud Computing for IT Pros: What Is Cloud ? https://blogs.technet.microsoft.com/yungchou/2010/12/17/cloud-computing-for-it-pros-26-what-is-cloud/, 2010. (Accessed May 18, 2017).

[334] Liang-Jie Zhang, Jia Zhang, Jinan Fiaidhi, and J. Morris Chang. Hot Topics in Cloud Computing. *IT Professional*, 12(5):17–19, 2010.

[335] Qi Zhang, Lu Cheng, and Raouf Boutaba. Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1):7–18, 2010.

[336] Xuan Xuejie Zhang, Nattapong Wuwong, Hao Li, and Xuan Xuejie Zhang. Information Security Risk Management Framework for the Cloud Computing Environments. *2010 10th IEEE International Conference on Computer and Information Technology*, (2007):1328–1334, 2010.

[337] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592, 2012.

[338] Radulescu Constanta Zoie, Balog Alexandru, Radulescu Delia Mihaela, and Dumitrache Mihail. A decision making framework for weighting and ranking criteria for Cloud provider selection. *2016 20th International Conference on System Theory, Control and Computing, ICSTCC 2016 - Joint Conference of SINTES 20, SACCS 16, SIMSIS 20 - Proceedings*, pages 590–595, 2016.

Appendix A

Glossary

Availability - This is the assurance that data will be accessible by authorised parties on demand.

Application Programming Interface (API) - An API is an easily consumable interface or communication protocol that simplifies access to features or data of an operating system, application, or service. APIs promote significant decoupling and dynamic binding of software capabilities.

Cloud Computing - This is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Customers - These are individuals or organisations that pay for and use the cloud services offered by a CSP.

Cloud risk assessment - The step by step, repeatable process used to produce an understanding of cloud risks associated with relinquishing control of data or management of services to an external service provider.

Cloud Service - This is a service that is deployed through the cloud computing infrastructure. The primary cloud services include SaaS, PaaS and IaaS.

Cloud Service Providers (CSPs) - These are cloud computing experts or vendors who offer some component of cloud computing through their infrastructures to other businesses or individuals.

Cloud supply chain - This is a network of individuals, organisations, resources, activities and technology involved in the provision, development, hosting, managing, monitoring or use of a cloud service.

Complex systems - A complex system is made up of a large number of interacting parts, who interact in non-linear ways and the whole is more than the sum of the parts.

Confidentiality - This is the assurance that only authorised parties can access data.

Continuous Monitoring - The process of maintaining ongoing awareness of the current cybersecurity state of a system throughout its lifecycle by collecting, analysing, alarming,

presenting and using other open-source information to identify anomalies, vulnerabilities and threats to the system as part of an incident response or risk management solution.

Delphi Method - This is a forecasting technique used to collect expert opinion objectively, with procedures that allow for anonymity over multiple iterations in a controlled manner.

Frequency of risk event - The number of times a risk event can happen in a year.

Infrastructure-as-a-Service (IaaS) - The IaaS service model is the foundation of all cloud services as it presents customers with virtualised resources (storage, servers and network) on which they can run their operating system, and build their application stack.

Impact - This is the potential loss associated with a risk item if the threat exploits the vulnerability.

Integrity - This is the assurance that only authorised parties can modify data.

Monte Carlo Simulation -This is a stochastic modelling tool which is used to provide estimates for complex problems where there are significant uncertainty.

Platform-as-a-Service (PaaS) - The PaaS service model refers to the delivery of a computing platform and solution stack as a service.

Probability of a risk event (without controls) - This is the chance that the identified threats can exploit the identified vulnerabilities.

Probability of a risk event (with controls) - This is the chance that the identified threats can exploit the identified vulnerabilities with the existing security controls in place.

Qualitative risk assessment - This method employs a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels(e.g., low, moderate, high).

Quantitative risk assessment - This method employs a set of methods, principles, or rules for assessing risk based on the use of numbers. It attempts to assign real numbers to assets, and assigns a dollar value to the impact of a threat on the asset should the risk materialise.

Risk - The effect of uncertainty on objectives.

Risk model - A risk model defines the risk factors to be assessed and the relationship among the risk factors.

Software-as-a-Service (SaaS) - SaaS is a model of software deployment whereby a CSP licenses an application to customers for use as a service on demand.

Supply Chain - A supply chain is a system of organisations, people, processes, information and technologies involved in the manufacture and distribution of a product or service from supplier to customer.

Systems Thinking - It is an approach to problem-solving that looks at problems in the context of a larger system made up of many components, instead of as an isolated challenge.

Threat - A threat is any circumstance or event with the potential to adversely impact organisational operations and assets, individuals, organisations or nation through an information system.

Transparency - This is the disclosure of security-related practices and controls to customers by cloud service providers and their suppliers.

Visibility of Security Controls - The discoverability of cloud supplier or provider security controls.

Vulnerability - This is any weakness in an information system, system security procedure, internal controls, or implementation that can be exploited by a threat source.

Z-score - The statistical measurement of a score's relationship to the mean in a set of scores. It measures how many standard deviations a score is above or below the population mean.

Appendix B

Coding, Description and Mapping of Security Factors

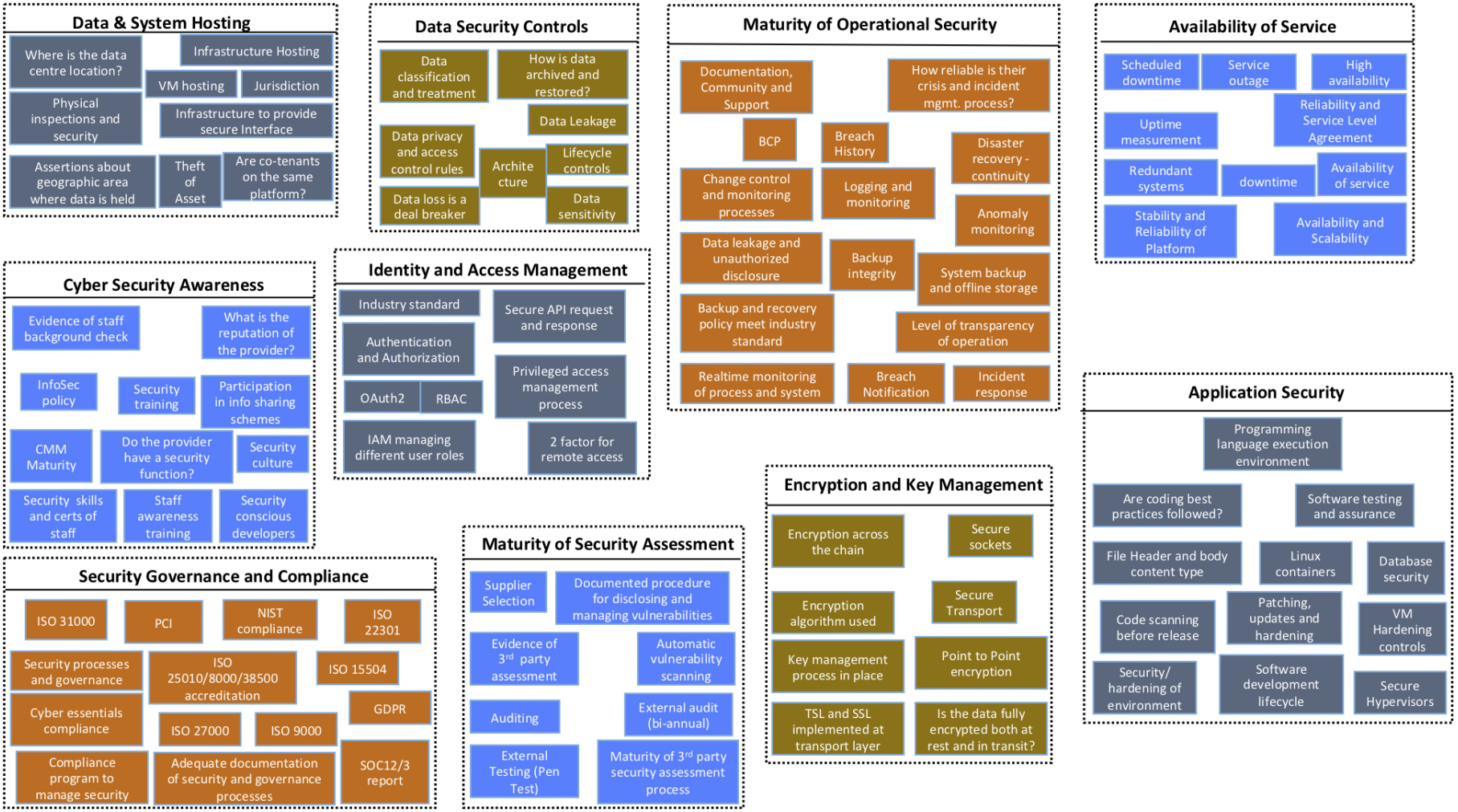


Figure B.1: Organising the security factors into target dimensions using Affinity Diagram

Table B.1: Description of the 52 security criteria for Cloud Supplier Assessment

No.	Security Factor	Subfactors	Description
1.	Availability of Service		
		Measure of downtime and uptime	A measure of the uptime commitment by the supplier and verification of their adherence to it.
		Reliability	How reliable is the cloud service offered by the supplier? Is the provider made aware of incidents that could affect the availability of their service in a timely fashion?
		SLA compliance	Assess the supplier's adherence to service commitments and key performance, requirements stated in the SLA.
		Change control outages	Auditing supplier outages, to confirm if unauthorised or unplanned changes caused them.
		Infrastructure & System redundancy	A review of the vendor's operational resiliency to service interruptions. Supplier implements multiple systems and processes to sustain, minimise and recover, operations in the event of an outage.
2.	Data & System hosting		
		Infrastructure & virtualisation secure hosting	Physical security of the server hosting the hypervisor, and proper management of the configuration and operation of the virtualised platform.
		Multi-tenancy	CSP is aware of the multi-tenancy arrangement of the supplier, and the controls put in place to ensure the segmentation and isolation of CSP data.
		Location/ Jurisdiction	A measure of supplier's compliance across the multiple jurisdictions in which, CSP data is processed. CSP data is not processed outside the agreed jurisdiction. This factor also looks to understand the logical and physical location of data at any given time.
		Physical Access security	Adequate controls are put in place to limit physical access to hosting facility to authorised users only.
3.	Data security controls		
		Data treatment	How is data processed when in possession of suppliers? How is data stored and transmitted within the cloud supplier infrastructure? Is the data seen by other third parties, unknown to the CSP?
		Classification of sensitive data	The supplier has detailed security documentation on the identification, classification and labelling of sensitive data.
		Data replication policies	What data replication processes are implemented within the supplier environment? Does the supplier apply similar controls to real-time and archived data for consistency?
		Disclosure of data leakage/ unauthorised access	Supplier keeps a proper accounting of authorised and unauthorised disclosure of data, and inform appropriate parties of related incident.
		Data availability and privacy policies	Supplier's data security and privacy policy follow an established framework and meet regulatory compliance requirements. Also, this policy meets CSP business needs and regulatory obligation.
		Data lifecycle controls	Supplier data lifecycle controls meet CSP needs. CSP ensures that the supplier has processes in place to execute the, six phases of data lifecycle management.

Table B.2: Description of the 52 security criteria for Cloud Supplier Assessment (contd)

No.	Security Factor	Subfactors	Description
4.	Maturity of security assessment		
		Regular vulnerability assessment & penetration testing	CSP has evidence that vendor conducts a regular security assessment of their physical and virtualised infrastructure.
		Internal / External auditing	Supplier engages the service of internal and external auditors to measure the effectiveness of its policies, procedures and implemented controls.
		Third party assessment process	Suppliers assess the risk and compliance of their third-party vendors and have controls in place to mitigate supply chain-related risks.
		Risk assessment & treatment	The supplier adopts an applicable risk assessment framework in assessing the impact and likelihood of risk events. The risk assessment process evaluates the risk of both the vendor and the cloud service.
		Subcontractor Selection and Management Process	Suppliers adopt a vendor selection system that enables them to identify, evaluate and select contractors that meet their security requirements.
5.	Maturity of Operational Security		
		Documented DR/BCP process	Suppliers have a service redundancy process in place to keep them in operation even after an impact to the primary infrastructure.
		Configuration management	The supplier has a strict configuration management process, which maintains the integrity of its systems throughout the system development lifecycle.
		Data breach detection & notification	The supplier has controls in place to detect and respond to data breaches. They notify customers and other impacted, businesses in a timely fashion about security incidents or a confirmed breach.
		Security incident handling and reporting	Availability of a security incident response plan, which outlines roles and responsibility for communicating and escalating an incident.
		Logging and monitoring	Controls are in place to monitor and log all user activity and actionable events. Supplier also has process in place to detect and respond to log errors.
		Transparency of security operation	The supplier is upfront about the security controls in place, resource, capacity, operational capability, potential risks, and data handling process.
		System backup & storage process	How transparent is supplier's backup and storage process? Where is the location of data backups (onsite, off-site)?
		Change control process	Evidence of the supplier having a coordinated, auditable and verifiable change management process that meet CSP needs.
		Malware Prevention	Defence-in-depth controls are in place to detect and protect customer data from malicious attacks.

Table B.3: Description of the 52 security criteria for Cloud Supplier Assessment (contd)

No.	Security Factor	Subfactors	Description
6.	Security Governance and Compliance		
		Compliance to legal, industry and regulatory standards	Assessing the vendor and its supply chains' compliance with legal, industry or regulatory standards. Does the supplier show the commitment to maintain the desired level of security to protect the business-critical processes?
		Independent review of security controls	Evidence of independently conducted audit of the supplier security controls in such a way that it provides greater transparency of their operation and compliance.
		Continuous monitoring	Supplier organisations should have an IT governance team that reviews their regulatory compliance at regular intervals and provides an update.
7.	Identity and Access Management (IAM)		
		Industry standard application controls (e.g. Oauth2)	Cloud supplier leverages a convergence of open standards to authenticate and, authorise users to access cloud services, e.g. the use of SAML, OpenID and, Oauth.
		Role-Based Access Control (RBAC)	The supplier provides evidence on the implementation of user access and revocation policies, least privilege controls and separation of duties.
		Multi-Factor Authentication (MFA)	Accessing customer data through supplier infrastructure is made available only through MFA, i.e. a combination of at least two different types of authentication, mechanism.
		Authentication, Authorization, and Accounting policies	The supplier has controls in place to prevent unauthorised access to customer, data, and every activity conducted in a customer environment is centrally logged.
		Secure remote access	Supplier implements security layers that address the secure transmission, physical protection, anomaly detection and analysis of user access to remote access servers.
8.	Encryption & Key Management (EKM)		
		Use of open encryption algorithms	The supplier makes use of the more secure open-source cryptography algorithms, such as AES and RSA. They avoid the use of proprietary encryption algorithms, which initially offer secrecy.
		Cryptographic key management process	The key management process allows CSP to securely create, store, use, and destroy their unique encryption keys, preventing the disclosure of sensitive data.
		Encryption at rest and in transit	Protecting data including log files, metadata etc., when in transit to the cloud, at rest, and in use. Supplier meets CSP data encryption requirement.
		Secure transport	The use of secure, standardised network transport protocol for the import and export of customer data e.g. SSL/TSL
		Point-to-point or end-to-end encryption	Supplier supports the tamper-proof transmission of sensitive data such as credit card information through their infrastructure.

Table B.4: Description of the 52 security criteria for Cloud Supplier Assessment (contd)

No.	Security Factor	Subfactors	Description
		Protecting the integrity of exchanged data	The supplier provides CSP with integrity monitoring for the data processed and/or stored within the supplier environment.
9.	Application Security		
		Secure coding best practice	Supplier adopts software coding safeguards that allow them to identify and address any security flaws during development before it is released.
		Secure Systems Development Life Cycle (SDLC)	The supplier adopts a good blend of processes, tools and technologies in the development and operation of their cloud software. They utilise maturity, models in determining areas where they need to improve.
		Static and dynamic source code scanning	Supplier utilises static and dynamic means to conduct vulnerability testing on the source and object code (binaries).
		Software testing/ assurance	Supplier undertakes application penetration testing to identify vulnerabilities that can be exploited by malicious actors.
		Virtual machine (VM) hardening controls	Supplier implements proper hardening and security controls for virtual machine instances. These controls include the use of firewall, HIPS, Antivirus, file integrity and log monitoring.
		Proactive software patches	The supplier has processes in place to scan for critical software updates and patches for development platforms and operating systems.
		Secure code execution environment	Suppliers adopt a formal coding best practice in the development of their application. This approach is secure and provides the ability to control the execution of the object code based on the specified functional requirements.
		File and content security	The supplier has controls that prevent, detect and respond to malicious threats by scanning file contents for signs of malware behaviour.
		Secure hypervisors and operating system containers	The supplier has controls in place to ensure secure intra and inter-host communication between virtual machines.

Table B.5: Mapping of Security Factors to Standards and Guidance

No.	Security Factor	Security Criteria	NIST SP800-53 Revision 3	ISO/IEC 27001:2013	COBIT 5.0	Shared Ass. 2017 AUP	CSA Guidance V3.0
1.	Availability of Service						
		Measure of Downtime vs. Uptime	SC-6				
		Reliability	CP-9	A.15.1.1		A.6	
		SLA compliance		A.18.2.3	DS1.3		
		change control outages	CM-3	A.12.1.2, A.15.2.2	AI6.1	G.1	
		Infrastructure & System redundancy	CP-2,CP-6, CP-7	A.11.2.4, A.17.2.1			
2.	Data & System Hosting						
		Infrastructure and virtualisation secure hosting	AC-20		AI3.3	V. 4	
		Multi-tenancy	AC-4, SC-7	A.7.3.1		E.5	Domain 1
		Location/Jurisdiction					
		Physical Access security	PE-2, PE-3, PE-4, PE-5	A.11.1.2, A.11.1.3	DS12.5, DS12.3	F.2 , H.7	Domain 7
3.	Data security controls						
		Data treatment		A 8.3		D.2 , D.5	Domain 3, 5
		Classification of sensitive data	RA-2, MP-3	A.7.2	PO2.3	I.4	Domain 5
		Data replication policies	SI-7	A.12.3.1	DS11.2, DS11.5		Domain 5, 7
		Disclosure of data leakage / unauthorised access	CM-8, CP-9, SC-7			D.5	Domain 9
		Data availability and privacy policies		A.18.1.4	DS11.5, DS11.6	D.4 , P.2	Domain 5
		Data lifecycle controls	MP-2, MP-4-5 ,MP-6, MP-7	A.8.2.3	DS11.4	D.3, D.8	Domain 5
4.	Maturity of security assessment process						
		Regular,vulnerability assessment and penetration testing	RA-3, RA-5, SI-2, SI-5, CA-2, CA-8	A.14.2.3, A.12.6.1		A.2, G.3, I.13, T.3	Domain 10
		Internal / External auditing	AU-1, AU-6	A.12.7.1	AI2.3	F.6	Domain 4, 10
		Third party assessment process	SA-12,CA-2-3	A.15.1, A.15.2, A.14.2.7, A.18.2.3	DS2.3, ME2.6	A.5, A.9	Domain 2
		Risk assessment and treatment	RA-3	A.17.1.3	PO4.8, ME4.5	A.2 , K.3	Domain 2
		Subcontractor Selection and Management Process		A.15.1.1,,A.15.2.1	AI5.2, DS2.3, AI5.3 -	A.7	
5.	Maturity of Operational Security						
		Documented DR/BCP process	CP-2, CP-6-7 ,CP-8, CP-9 -10	A.17.1.1, A.17.1.2	DS4.2, PO9.4	K.1	Domain 7
		Configuration management	CM-3		DS9		
		Data breach detection & notification	SI-5	A.16.1.2			
		Security incident handling & reporting	AU-6,IR-6,IR-4	A.16	DS5.6, DS8	J.1-7,P.8	Domain 9
		Logging and monitoring	AU-3, AU-6, AU-9, AU-1, AU-12, AU-14	A.9.2.5, A.16 ,A.12.4.2	DS1.5, DS13.3	H.9 ,I.12, O.1	
		Transparency of security operation		A.16.1			
		System backup and storage process	CP-9	A.12.3.1		K.5	
		Change control process	CM-3, CM-5, SA-10	A.12.1.2	AI6.1	G.1	
		Malware Detection and Prevention	AT-2, SI-3, SC-5,	A.12.2.1, A.11.1.4 ,A.13.1.1	DS5.9	N.4, N.6, T.1	Domain 9

Table B.6: Mapping of Security Factors to Standards and Guidance (contd)

No.	Security Factor	Security Criteria	NIST SP800-53 Revision 3	ISO/IEC 27001:2013	COBIT 5.0	Shared Ass. 2017 AUP	CSA Guidance V3.0
6.	Security, Governance and Compliance						
		Compliance to legal, industry and regulatory standards	CA-9	A.18.2.2	PO3.4, PO4.8, ME3.1	A.3	Domain 3, 4
		Independent review of security controls (e.g. SOC2 Type I & II)	AC-1, MP-1, SC-1	A.12.7.1, A.18.2.1	ME4.7		
		Continuous,monitoring & reporting of infrastructure compliance	CA-7	A.18.1		L.2 , A.12.6	Domain 10
7.	Identity and Access Management (IAM)						
		Industry standard application/API access controls (e.g. Oauth2)	AC-1	A.9			Domain 10
		Role-Based Access Control (RBAC)	AC-2, AC-3, AC-6, CM-5	A.9.2.2			Domain 12
		Multi-Factor Authentication (MFA)	AC-3	A.9.4.1		H.8	
		Authentication,Authorization and Accounting policies	AC-1-2, IA-2, IA-4, IA-8, AC-5	A.9.2.4, A.9.4.2 -4.3 ,A.9.1.3, A.9.2.1	DS5.4, DS5.5	H.1, H.3	Domain 10, 12
		Secure remote access	AC-3, AC-6, AC-17	A.6.2.2, A.9.4.5			
8.	Encryption and Key Management						
		Use of open encryption algorithms	SC-13	A.12.6.1		D.5, I.9	Domain 11
		Cryptographic key management process	SC-12, SC-17	A.10.1.2	DS5.8	D.5	Domain 11
		Encryption at rest and in transit	PE-4	A.9.1.2, A10.1.1		D.3 , D.6, N.8	Domain 5
		Secure Transport (SSL/TSL)	SC-11, SC-8	A.14.1.3		D.7	
		Point-to-point encryption		A.10.1.1		D.7	Domain 11
		Protecting the integrity of exchanged data	CA-3, PE-17, SC-8,SI-7,	A.13.2.2, A.14.1.3	DS5.11, PO2.4	D.3, D.6	Domain 3, 5
9.	Application Security						
		Secure coding best practice	SA-3, SA-15, SA-17	A.6.2	AI7	G.8	Domain 10
		Secure Systems Development Life Cycle (SDLC)	SA-3, SA-10, SC-2	A.12.6.2, A.14.2, A.12.1.4,	AI2.4	I.2,I.16, U.1	Domain 10
		Static and dynamic source code scanning		A.12.2.2, A.12.2.1		G.3 , I.7, I.8	Domain 10
		Software testing/assurance	CA-2, SA-11, SI-10	A.12.7.1, A.14.2.8	AI2.8, AI7.4	I.8	
		Virtual Machine (VM) hardening controls				V. 4	
		Proactive software patches	SI-2	A.12.6	AI2.6, AI2.10	G.2	
		Secure code execution environment	AC-3, AC-6, CM-5, SI-3	A.11.1.5, A.11.2.7 A.11.2.9		F.3	Domain 10
		File and content security	SA-15(9)	A.14.3.1	AI2.4		Domain 5, 10
		Secure hypervisors and operating system containers				V. 4	

Appendix C

CUREC Approvals and Research Participant Invitation letters

SOCIAL SCIENCES & HUMANITIES
INTER-DIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

8 March 2016

Olusola Akinrolabu
Department of Department of Computer Science

Dear Olusola Akinrolabu,

Research Ethics Approval (CUREC 1A)
Ref No: R44459/RE001

Title: Supply Chain Risk in Cloud Computing

The above application has been considered on behalf of the Social Sciences and Humanities Inter-divisional Research Ethics Committee (IDREC) in accordance with the procedures laid down by the University for ethical approval of all research involving human participants.

I am pleased to inform you that, on the basis of the information provided to the IDREC, the proposed research has been judged as meeting appropriate ethical standards, and accordingly approval has been granted.

Should there be any subsequent changes to the project, which raise ethical issues not covered in the original application, you should submit details to the IDREC for consideration.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager and Secretary SSH IDREC

cc: Sharon Lloyd

SOCIAL SCIENCES & HUMANITIES
INTER-DIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

21 February 2017

Olusola Akinrolabu
Department of Computer Science

Dear Olusola,

Research Ethics Approval (CUREC 1A)
Ref No: R50232/RE001

Title: Cyber Supply Chain Risks in Cloud Computing: The Effect of Transparency on Risk Assessment

The above application has been considered on behalf of the Social Sciences and Humanities Inter-divisional Research Ethics Committee (IDREC) in accordance with the procedures laid down by the University for ethical approval of all research involving human participants.

I am pleased to inform you that, on the basis of the information provided to the IDREC, the proposed research has been judged as meeting appropriate ethical standards, and accordingly approval has been granted.

Should there be any subsequent changes to the project, which raise ethical issues not covered in the original application, you should submit details to the IDREC for consideration.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager and Secretary SSH IDREC

cc: Andrew Martin
Sharon Lloyd

SOCIAL SCIENCES & HUMANITIES
INTERDIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

5 December 2017

Olusola Akinrolabu
Department of Computer Science
University of Oxford

Dear Ms Akinrolabu,

Research Ethics Approval (CUREC 1A)
Ref No: R54943/RE001

Title: Cyber Supply Chain Risks in Cloud Computing: The Effect of Transparency on Risk Assessment of SaaS

The above application has been considered on behalf of the Social Sciences and Humanities Interdivisional Research Ethics Committee (IDREC) in accordance with the procedures laid down by the University for ethical approval of all research involving human participants.

I am pleased to inform you that, on the basis of the information provided to the IDREC, the proposed research has been judged as meeting appropriate ethical standards, and accordingly approval has been granted.

Should there be any subsequent changes to the project, which raise ethical issues not covered in the original application, you should submit details to the IDREC for consideration.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager and Secretary SSH IDREC

cc: Prof Andrew Martin, Dr Steve New, Sharon Lloyd

Departmental Research Ethics Committee
ethics@cs.ox.ac.uk
Chair: Professor Andrew Martin
Secretary: Katherine Fletcher

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

6 September 2018

Olusola Akinrolabu
Department of Computer Science

Dear Mr Akinrolabu,

Research Ethics Approval

Ref No: SSD/CUREC1A CS_C1A_18_026

**Title: Cyber Supply Chain Risks in Cloud Computing:
Effect of Transparency on Risk Assessment of SaaS**

The above application has been considered on by the Computer Science Departmental Research Ethics Committee (DREC), on behalf of the Social Sciences and Humanities Inter-divisional Research Ethics Committee (IDREC) in accordance with the procedures laid down by the University for ethical approval of all research involving human participants.

I am pleased to inform you that, on the basis of the information provided to the DREC, the proposed research has been judged as meeting appropriate ethical standards, and accordingly approval has been granted.

Should there be any subsequent changes to the project, which raise ethical issues not covered in the original application, you should submit details to the IDREC for consideration.

Yours sincerely,

Katherine Fletcher
Computer Science DREC Secretary

cc: Sharon Lloyd, Computer Science Departmental Administrator
(sharon.lloyd@cs.ox.ac.uk)

Send Attach Protect Discard

From: Olusola Akinrolabu
Sent: 28 September 2018 11:28:51
To: olusola.akinrolabu@cs.ox.ac.uk
Cc: olusola.akinrolabu@cs.ox.ac.uk
Subject: RE: Academic Case Study Invitation - Calling SaaS providers to trial our cloud risk assessment model.

Hello,

We are sending this email to you because you have once responded to our survey on cloud risk assessment. Thank you.

Over the past 24 months, we have conducted a series of studies in relation to cloud risk assessment and have introduced several novel concepts for assessing cloud provider risks. We Identified a significant cyber supply chain gap in both literature and practice, one which has prevented cloud providers from seeing the 'big picture' when addressing cloud risks. Furthermore, seeing that ***"you cannot effectively manage what you can't measure"***, many organisations have fallen victim of supply chain related incidents, due to indirect attacks on their suppliers.

As a result of the above, we have recently proposed and developed the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model which is supported by supplier security assessment and supply chain mapping. The CSCCRA is currently targeting cloud providers, particularly SaaS CSPs, who rely on an increased number of suppliers to deliver a cloud service.

To validate the efficiency, effectiveness and usefulness of the CSCCRA model, we recently conducted a workshop with industry experts and members of academia, where the model was used in assessing the risks of a fictional company. Here a series of improvements were suggested, all which have now been implemented. We also took our validation to a next level, by conducting our first case study with a not-for-profit cloud provider and the feedback was positive.

Therefore, we are calling on all SaaS CSPs who are interested and will like to trial our model to reach out to us. There are lots of benefits in using our model for your next assessment (see below). One of the common feedbacks we have got is around the holistic nature of the model, and how it provides risk assessors and stakeholders estimating the value of risk with a big picture and a deeper understanding of the underlying architecture of the cloud service.

Please see the attached poster for more information on the risk assessment process, and the "why" for using our model. If this is not for you, but you believe another organisation could take advantage of it, kindly help pass this invitation along to them.

We appreciate your assistance in this regard and hope you will find the approach valuable to your business.

Many thanks

Olu

Olusola Akinrolabu
Cyber Security CDT
University of Oxford | Kellogg College
Addr: Department of Computer Science, Robert Hooke Building, Parks Road, Oxford OX1 3PR

The benefits to participating CSPs

Some of the benefits of participating in this study include:

1. Each participating SaaS CSP will get the opportunity to go through the risk assessment of their cloud service, analyse their supply chain, identify weak suppliers and receive a quantitative risk result in dollar terms.
2. The identification of potential weak spots in the supply chain through a dynamic model, such as the CSCCRA helps CSPs capture the vulnerability of their cloud service and promotes proactive mitigation of risks.
3. The graphical representation of the inherent risk in the supply chain helps to counter any documented biases in risk estimation and decision-making. It also helps in reducing the cognitive load involved in the estimation of risk factors.

Send Discard Draft saved at 14:00

Delphi Study - Invitation Letter

Page 1: Study Title: Cyber Supply Chain Risks in Cloud Computing: The Effect of Transparency on Risk Assessment.

Ethics Approval Reference: [R54943/RE001]

Invitation to participate in a Delphi Study - December 2017

An opportunity to contribute to research in identifying risk factors that can be used to rate cloud service suppliers/vendors.

Dear Sir/Ma,

I am a DPhil student at the University of Oxford, Computer Science Department. My DPhil research looks at the cyber supply chain risk assessment gap in cloud services, with the aim of investigating the impact of cloud provider transparency in addressing this gap. My research work is supervised by Professor Andrew Martin of the Computer Science Department and Dr Steve New from the Saïd Business School (SBS). This research is funded by the Engineering and Physical Sciences Research Council (EPSRC).

The analysis of our just concluded survey showed that cloud providers follow a distorted and incomplete process when selecting suppliers for critical aspects of their service. With about 90% of modern cloud applications (SaaS), assembled from third-party components, we uncovered a gap between best practices and mainstream practices when it came to cyber supply chain risk management. The notion of cloud decisions made based on functionality and cost seems to be weakening the security posture of cloud services, opening up less matured organisations to cyber attacks, and such attack magnified into the broader supply chain.

At this junction, our research work has reached the stage where we need to seek valuable input from cloud and information security professionals on the reliability and security factors cloud

providers should consider when choosing suppliers for the components of their cloud service. This stage of the research will be conducted as a Delphi study, where respondents will be part of a focus group but will provide their feedback to the researcher anonymously in about three iterations. If you agree to take part, a questionnaire will be sent to you, detailing a cloud provider's supply chain, and you will be asked to help the cloud provider determine which security, process, and/or reliability factors are worth considering when assessing the risk of their suppliers. This acts as a scientific means of collecting the information necessary to rate suppliers involved in the delivery of a cloud service. As part of our proposed cloud supply chain risk assessment model, we included a decision support analysis model, which looks to address the cloud supplier selection gap. The aim of the decision support model is to identify cloud suppliers with weak security controls or processes, and are readily susceptible to a cyber attack or has a high risk of failure.

This opportunity to contribute to academic research has reached you either because you signified interest to take part in our future study when you participated in our earlier research, or through your membership of a recognised Information Security Community of interest. In case you received this from multiple communities you belong to, I apologise and will appreciate if you could respond to just one of them. Completion of the questionnaire should take no more than 20 minutes. The responses from the first round will be analysed, and the collective feedback sent back to you for further scoring and comment on any emerging consensus from fellow professionals. In the second, and possible, third rounds the completion time is a lot shorter as you are being asked whether you agree or disagree with the emerging consensus.

Eligibility criteria for completion of the questionnaire

Through your experience in cloud computing and information security, many of you will meet the requirements. Ideally, we are looking for those with a broad information security, risk assessment, cloud computing, or supply chain background, who might have been involved in one or more of the following activities:

- Selecting supplier for a cloud service
- Information security risk assessment
- Mapping the supply chain/ value chain of a cloud service
- Threat modelling and attack surface analysis
- Governance, Risk and Compliance

Expression of interest to Participate

I am interested in participating in this research, I meet the eligibility criteria and I would like to receive a full participant information and consent form.

- Yes
- No

If you ticked “Yes”, please provide us with your email address and we will send you a copy of the Participant Information Sheet (PIS), which includes a consent form. The PIS goes into more detail about the study and allows you to ask questions before participating. However, if you think you do not meet the criteria stated above, but know of someone else who is eligible, but may not have received this, please kindly send them a copy of this letter.

We appreciate your assistance and do hope you can find this study stimulating and can add your valuable contribution to the research.

Yours faithfully,

Olusola Akinrolabu

DPhil Student, University of Oxford

Olusola.akinrolabu@cs.ox.ac.uk

Cyber Supply Chain Risks in Cloud Computing – Bridging the Cloud Risk Assessment Gap

O. Akinrolabu, S. New, A. Martin

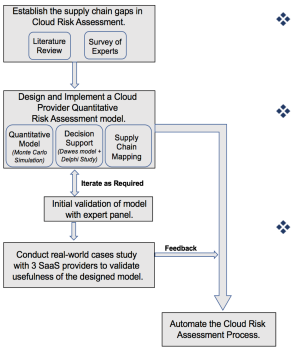
UNIVERSITY OF OXFORD

Cloud risk assessment gap

Security risks associated with the cloud's multi-tenancy, automation, vendor lock-in, and system complexity continues to be on the rise. Assessing and managing these risks can be a challenge due to the increased numbers of parties, devices and applications involved in cloud service delivery.

In a recent study conducted with cloud experts, we discovered how current risk assessment methods were unable to cope with the dynamic nature of the cloud, a gap linked to their failure to consider the inherent risk of the supply chain. This challenge is further exacerbated by the lack of cloud provider transparency and limited visibility of security controls.

Research Methodology & Progress



- We have developed a prototype quantitative cloud risk analysis model based on Monte Carlo simulation.
- We also carried out a Delphi study with cloud experts to identify security factors for our multi-criteria decision support system.
- We have recently completed the development of an automated supply chain mapping tool using a graph database platform.

CSCCRA: An Improved cloud risk assessment model

To address the above gap, we developed the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model which is supported by decision support analysis and supply chain mapping in the identification, analysis and evaluation of cloud risks.

The CSCCRA model is currently targeted at SaaS providers and follows a systematic approach to assessing cloud risks.

The five essential elements of a Cloud Supply Chain

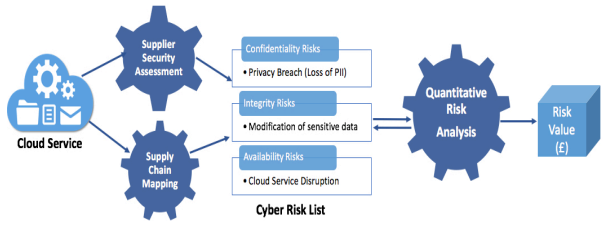
Delphi Study

A group of fifteen (15) experts were tasked with identifying security factors for cloud supplier assessment.

This group achieved consensus on nine (9) security target dimension, and they are:

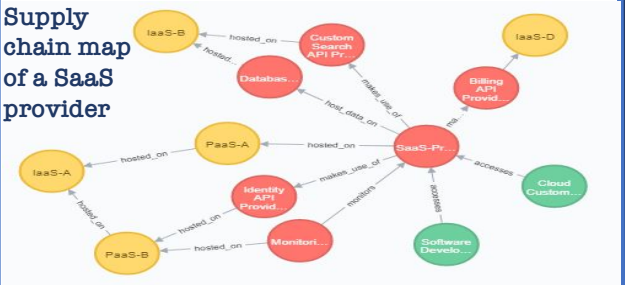
- Maturity of Operational Security
- Identity and Access Management
- Availability of Service
- Data security controls
- Application Security
- Encryption and Key Management
- Data & System hosting
- Data security controls
- Maturity of security assessment
- Security Governance & Compliance

How the CSCCRA Model works



- Decompose the cloud application into its component services and map out the supply chain.
- Assess the security of the supplier of each service component using a multi-criteria decision support system.
- Identify the weak link(s) within the chain and draw a comprehensive list of cloud security risks.
- Stakeholders make reasonable estimates of risk values.
- Input risk values to CSCCRA quantitative simulation tool, to arrive at the risk value in monetary terms.

Supply chain map of a SaaS provider



Open invitation for collaboration

The next phase of our research is to conduct at least 3 case Studies, where we will be using the CSCCRA model to analyse the risk of cloud providers.
We believe this exercise will provide SaaS providers with an opportunity to step back cognitively from their usual approach to risk assessment and fundamentally question and rethink their established interpretations of cloud risks.

For further discussions or enquiries, please contact Olu Akinrolabu (olusola.akinrolabu@kellogg.ox.ac.uk)

Recent Publications

- Akinrolabu, O., New, S. and Martin, A., 2018. Cyber supply chain risks in cloud computing–bridging the risk assessment gap. Open Journal of Cloud Computing (OJCC), 5(1), pp 1-19.
- Akinrolabu, O., New, S. and Martin, A., 2018, August. Cloud Service Supplier Assessment: A Delphi Study. In Innovative Computing Technology (INTECH), 2018 Eight International Conference. IEEE.
- Akinrolabu, O., New, S. and Martin, A., 2018, October. CSCCRA: A Novel Quantitative Risk Assessment Model for Cloud Service Providers. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp.). Springer.

CENTRE FOR DOCTORAL TRAINING in CYBER SECURITY

EPSRC Engineering and Physical Sciences Research Council

Appendix D

Survey Questionnaires and Results

Saïd Business School
University of Oxford

Park End Street, Oxford OX1 1HP, UK
T +44 (0)1865 288800
www.sbs.oxford.edu

INVESTIGATING THE CLOUD SUPPLY CHAIN

WHAT ARE THE CYBERSECURITY AND RELIABILITY ISSUES IN CLOUD COMPUTING?

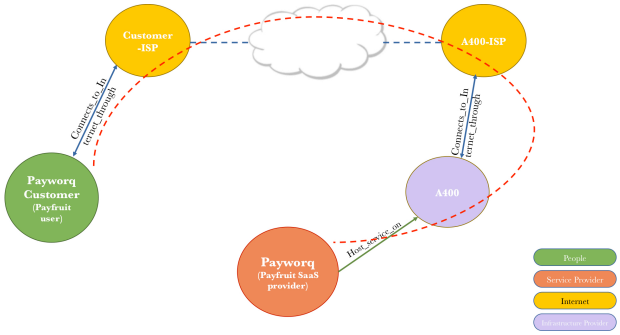
We are researching how firms are approaching questions of visibility and transparency in Cloud Computing. We would like to get your opinion about this **FICTIONAL** story – to help us understand the key issues. It will only take a few minutes, and we will email you a free copy of our upcoming report, which will contain the findings of this research.

Here is the story:

--♦♦--

Payworq Ltd offers payroll-processing software (*PayFruit*), which runs as Software-as-a-Service (SaaS). Its move to the cloud was due to an increased demand for *PayFruit*, from small businesses and start-ups. Payworq needed an Infrastructure as a Service (IaaS) provider to host its growing service, and it looked for cloud service providers (CSP) from provider websites and attending exhibitions and trade events. Eventually, it selected A400 Ltd based on its reputation and on its promise of flexibility, rapid scalability, redundancy and compliance to standards.

Recently, the *PayFruit* service was offline for approximately four hours as a result of a power outage at the A400 Ltd.'s Internet Service Provider (ISP). The situation was very damaging for Payworq; several of its customers were unable to pay their staff on time, and it now faces financial penalties.



As part of its incident management process, Payworq has arranged a meeting with the A400 to try to ensure that this incident does not happen again. It wants to know more about the 'supply chain' of other providers which may lie behind A400's offering. They want to follow this up with a comprehensive risk assessment of the benefits and vulnerabilities of their cloud solution.

--♦♦--

Over the page, we'd like you your opinion on two critical issues:

- What information should Payworq ask for?
- How much should A400 be prepared to tell

What information should Payworq ask for?

Cloud computing services are often sold on the idea that customers don't need to know the exact detail of the operations of their Cloud Service Provider's operations: but is this a good idea?

- How much should A400 be prepared to tell?

  Providers are often reluctant to reveal too much about their operations - even to customers. What are the issues about being completely transparent about your operations?

Please give us your email address, so we can send you a copy of our forthcoming report. All information will be treated as confidential, and your response and details will not be used for any other purposes beyond this research, or passed to any third party. Neither you nor your firm will be identified in our report.

Email:	

Mr. Olusola Akinrolabu, Doctoral Student, Kellogg College, Centre for Doctoral Training in Cybersecurity University of Oxford, olusola.akinrolabu@kellogg.ox.ac.uk
Dr. Steve New, Fellow, Hertford College, Associate Professor of Operations Management, Saïd Business School, University of Oxford http://www.sbs.ox.ac.uk/community/people/steve-new, steve.new@sbs.ox.ac.uk

Stage 1 Result - Detailed description of the Eight (8) Transparency features used for CSP comparison criteria

#	Transparency Feature	Description
1.	Architecture	Under Architecture, we aim to find details of the high-level architecture of the CSPs cloud offering. We look out for technical specifications of the network, security, storage and server infrastructures that deliver the cloud service. For example, a SaaS provider could mention how their server infrastructure is protected from malicious traffic and the high availability functionality of their cloud solution.
2.	Technology/Partners	Here, we are looking to see if SaaS providers mention their IaaS hosting provider and in the case where they own their infrastructure, their hardware, software and internet service providers. For example, Capsule CRM publish that their servers are hosted in Amazon's data centres while Fifosys a SaaS and IaaS provider, also have companies like Cisco, Citrix, Equinix and Microsoft as their partners.
3.	Datacentre Location	The choice of datacentre location as one of the criteria is to help customers in determining the jurisdiction under which their data is stored. A cloud vendor that hosts their service within the UK assures the customer that they will be protected under the EU data protection directive.
4.	Security Features	Here we look out for the mention of security controls implemented by the CSP to protect their cloud service. Some of the features we look out for include encryption, (physical, server and application) security, high-availability, password protection, etc.
5.	IT-related compliance certification	With IT certification, we look for SaaS providers, whose organisation has gone beyond leveraging their providers' accreditation, to obtain theirs. Certification like ISO27001, Payment Card Industry (PCI) and cyber essentials are common amongst these providers.
6.	Advertised SLA	With SLA, we look out for CSPs that have explicitly provided details on the availability of their product and how quickly they expect to respond in the event of an incidence. It is also useful for customers to know what the average uptime of the cloud service has been over the year, and if the provider has a track record of meeting SLA.
7.	Disaster Recovery/ Business Continuity	Here we look for CSPs that have mentioned data backup, RPO (Recovery Point Objective) and RTO (Recovery Time Objective) on their website. We also considered where CSP provided details of their failover datacenter for resiliency.
8.	Monitoring/Support	With monitoring and support, we aimed to find details of the support helpline, and the mode of operation (e.g. 24/7). We looked out for alert and notification methods deployed by the CSP to provide their customers with service related information.

Stage 1 Result - Comparison of 25 SaaS providers taken from Cloudscape CSP list

SaaS Cloud Provider comparison based on Transparency feature											
SaaS Cloud Provider	**Architecture (Yes/No)**	**Technology/ Partners (Yes/No)**	**Data center location (Yes/No)**	**Security features (Yes/No)**	**IT-related compliance certifications (ISO 27001, PCI-DSS, ITIL etc.) (Yes/No)**	**Other cloud offering (PaaS, IaaS & Others)**	**Private, Public, & Hybrid**	**Advertised Service Level Agreement (SLA) (Yes/No)**	**Disaster Recovery/ Business Continuity (Yes/No)**	**Monitoring/Support (Yes/No)**	**Scoring (No. of Yes) Maximum=8**
Online workspace sub-group											
CSP1	Yes	Yes	Yes	Yes	Yes	IaaS and PaaS	All	No	Yes	Yes	7
CSP2	Yes	Yes	Yes	Yes	Yes	IaaS	All	Yes	Yes	Yes	8
CSP3	No	Yes	Yes	Yes	Yes	IaaS and others	All	No	Yes	Yes	6
CSP4	No	Yes	Yes	Yes	Yes	IaaS and others	All	Yes	Yes	Yes	7
CSP5	Yes	Yes	Yes	Yes	Yes	N/A	All	Yes	Yes	Yes	8
Finance/ERP sub-group											
CSP6	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
CSP7	No	No	No	Yes	No	N/A	public	No	No	No	1
CSP8	No	Yes	Yes	Yes	Yes	IaaS	All	No	Yes	Yes	6
CSP9	No	No	No	No	No	N/A	public	No	No	No	0
CSP10	,No	No	No	No	No	N/A	public	No	No	No	0
Human Resources (HR) sub-group											
CSP11	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP12	No	Yes	No	Yes	No	N/A	public	Yes	No	Yes	4
CSP13	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
CSP14	Yes	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP15	No	No	No	No	No	N/A	public	No	No	No	0
Customer Relationship Management (CRM) sub-group											
CSP16	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP17	Yes	Yes	Yes	Yes	Yes	N/A	public	No	No	Yes	6
CSP18	No	Yes	No	No	No	N/A	public	No	No	Yes	2
CSP19	No	Yes	Yes	Yes	No	IaaS	public	Yes	Yes	Yes	6
CSP20	No	No	No	Yes	No	N/A	public	No	No	Yes	2
Collaboration sub-group											
CSP21	No	No	No	Yes	No	N/A	public	No	No	No	1
CSP22	Yes	Yes	Yes	Yes	Yes	N/A	public	Yes	Yes	Yes	8
CSP23	No	Yes	Yes	Yes	No	N/A	All	Yes	Yes	Yes	6
CSP24	No	Yes	Yes	Yes	Yes	IaaS and PaaS	All	Yes	Yes	Yes	7
CSP25	No	Yes	Yes	Yes	Yes	N/A	Public	Yes	Yes	Yes	7

Section B: Delphi Study Questionnaire

Scenario

A Customer Relationship Management (CRM) SaaS provider has incorporated several components into its cloud offering. A list of cloud suppliers whose services were enlisted includes a platform provider PaaS-A, whose service is hosted on IaaS-A, and a SQL database provider (SQL DB) whose service is hosted by IaaS-B. The Implementation of the CRM application also makes use of four API providers for services such as customer billing, custom `social search', monitoring, and Identity & Access Management (IAM). As shown in Figure 1, the IAM and monitoring API providers host their applications using the platform provided by PaaS-B, whose service is hosted on IaaS-A infrastructure.

The CRM provider is now in the process of assessing the risk of their cloud service, but before they begin the risk analysis phase, they will like to conduct a security assessment of their 3rd party providers. The purpose of this assessment is to identify which member of the supply chain has the weakest security and reliability posture, and who poses the greatest risk to their cloud service.

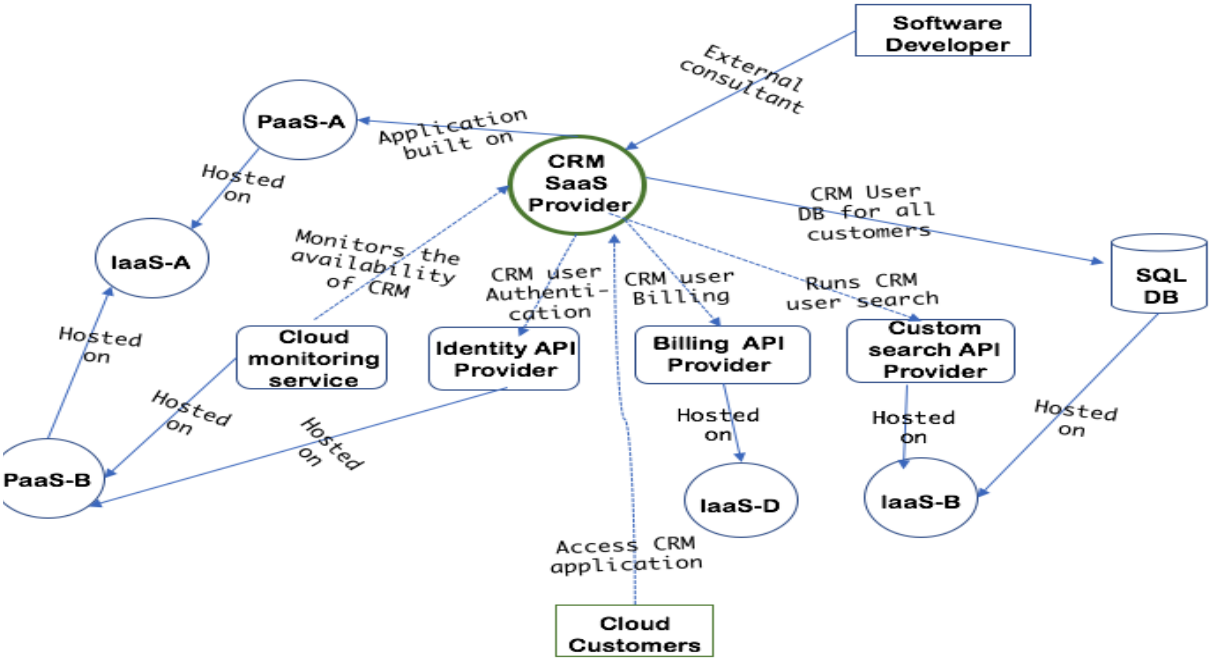


Figure 1: The Supply Chain of the CRM SaaS application

Task

Putting yourself in the position of the CRM provider, what security, process, and/or reliability

factors will you be looking out for in each component vendor to determine if they pose a risk to your cloud service. You are encouraged to draw upon your experiences, and use any historical data, research, or other available resources you find useful to respond to the questions.

Please provide us with at least 7 factors you will consider for each of the component providers.

Factor 1: ✱ *Required*

Factor 2: ✱ *Required*

Factor 3: ✱ *Required*

Factor 4: ✱ *Required*

Factor 5: ✱ *Required*

Factor 6: ✱ *Required*

Factor 7: ✱ *Required*

Any other factors:

UNIVERSITY OF OXFORD
Cyber Security CDT, Dept of Computer Science
Robert Hooke Building, Parks Road, Oxford OX1 3PR
Olusola.akinrolabu@kellogg.ox.ac.uk, 07875013532
RESEARCH: CYBER SUPPLY CHAIN RISK ASSESSMENT (CSCCRA)

CSP Risk Assessment Questionnaire

Date:
Organisation:

Security Assessment

Q1. Are you hosting your SaaS application with a cloud provider?

Q2. Do you manage the virtual machines, or is provider responsible for server management?

Q3. Did you build provider and geographical redundancy into the solution hosting the SaaS application?

Q4. Where is customer Personal Identifiable Information (PII) stored?

Q5. Do you store customer credit card data?

Q6. Is the Provider payment card industry (PCI) compliant?

Q7. Do you integrate with an Identity and access management (authentication) provider?

Q8. Do you have role-based access control (RBAC) in place for developers and administrators?

UNIVERSITY OF OXFORD
Cyber Security CDT, Dept of Computer Science
Robert Hooke Building, Parks Road, Oxford OX1 3PR
Olusola.akinrolabu@kellogg.ox.ac.uk, 07875013532
RESEARCH: CYBER SUPPLY CHAIN RISK ASSESSMENT (CSCCRA)

Q9. Have you implemented controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?

Q10. Does the application support Multi-factor authentication (MFA)?

Q11. Do you have change and configuration management in place?

Q12. Is data encrypted at rest, in transit or both?

Q13. Do you have an external backup of the application data? Where?

Q14. Do you restrict, log and monitor access to your information security management systems?

Q15. Do you use an encrypted channel for backup and restore operations?

Q16. Where are the server and application logs stored?

Q17. Where do you store the software code backup?

Q18. Have you implemented a web application firewall (WAF) and other threat detection systems for your SaaS application?

UNIVERSITY OF OXFORD
Cyber Security CDT, Dept of Computer Science
Robert Hooke Building, Parks Road, Oxford OX1 3PR
Olusola.akinrolabu@kellogg.ox.ac.uk, 07875013532

Q19. Have you conducted, or do you plan to hold regular penetration tests and vulnerability scans of the SaaS environment?

Q20. Do you review your applications for security vulnerabilities and address any issues before deployment to production? If yes, please state how.

Supplier Information

Q21. Using the table below, provide us with a list of the vendors whose application/API is integrated into your software? E.g. DNS, Storage, Authentication, Backup, Log management, Database, Performance monitoring, Payment, Firewall and Threat Protection.

Q22. Identify the function of each of the application listed above and provide a web address for each vendor? Also, confirm if they process or store customer or application data.

Q23. Please provide us with a data flow diagram, showing how the individual components of the application are integrated?

UNIVERSITY OF OXFORD
Cyber Security CDT, Dept of Computer Science
Robert Hooke Building, Parks Road, Oxford OX1 3PR
Olusola.akinrolabu@kellogg.ox.ac.uk, 07875013532

Vendor e.g. AWS	**Service** IaaS	**Location** UK	**Website**	**Data processing** Yes	**Data Storage** Yes

Appendix E

Assessing Cloud Risks using the CSCCRA Web Application

In the following paragraphs, we will walk through the assessment process, using the screen-shots taken from CSP-C's evaluation of the software application. We referred to the CSP in this evaluation as CSP-SW-Trial and followed the steps listed below in assessing the risk of the cloud service (CSP-SW-SaaS).

1. Decompose the cloud application into its component services and map out the supply chain.
2. Assess the security of the supplier of each service component using a multi-criteria decision support system.
3. Identify the weak link(s) within the chain and compile a comprehensive list of cloud security risks.
4. Enable stakeholders within the CSP to make reasonable estimates of risk values.
5. Input risk values to the CSCCRA quantitative simulation tool to arrive at the risk value in monetary terms.

E.1 CSP-SW-Trial Registration and Login

Figure E.1, shows the participants creating a new CSP record (CSP-SW-Trial), including a username and password. The password is stored in the database using a salted MD5 hash, which provides a simple form of confidentiality protection for the user passwords. On the right side of the diagram, the user (SAdmin) login to the web application and is presented with the home page (see Figure E.2). The home page provides the CSP stakeholders with information about the model and also has a link to one of our research papers, which goes into greater detail on the process of using the model to assess cloud risks. Seeing that CSP-C participants were already familiar with the model, they progressed to the assessment.

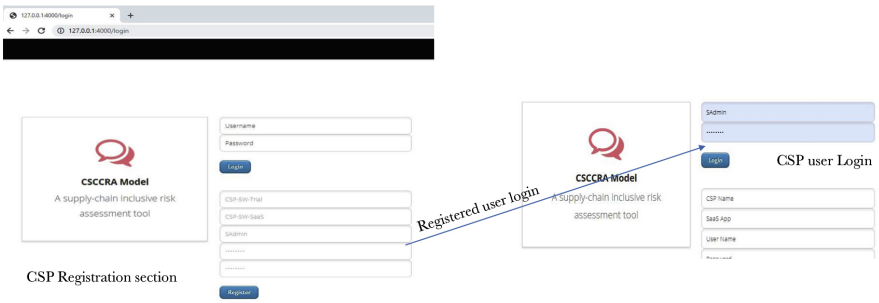


Figure E.1: CSP-SW User Registration and Login Page

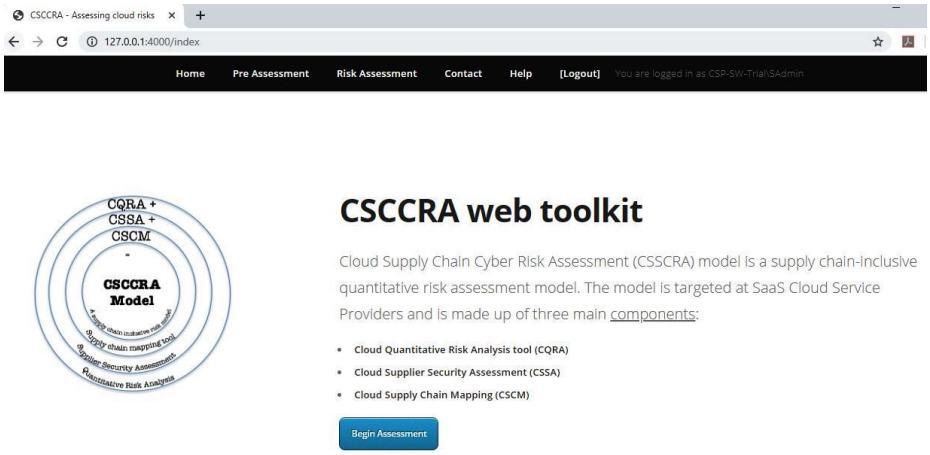


Figure E.2: CSP-SW-Trial Home Page

E.2 Supplier Identification and Supply Chain Mapping

By clicking the "Begin Assessment" button, the participants were presented with the Pre-Assessment page, from where they could pick one of three options. Going by the steps of the CSCCRA model, the CSP is to "decompose the cloud application into its component services and map out the supply chain", which is what the participants did. Click on the Identify SaaS components, they entered each component of the supply chain, identifying their service type, supplier and criticality (see Figure E.3).

On completing the component identification, they proceeded to map the supply chain, identifying how each component linked to the other (source and destination nodes) and their relationship types. They went through each component and in some cases, identified 2nd tier suppliers. At the end of the task, they clicked on the show map, which produced the diagram in Figure E.4. Also by clicking, "show connections" the table to the left of the diagram is produced. The use of a visual structural model helps to illustrate the interdependencies between the components and accurately visualise the cloud information flow.

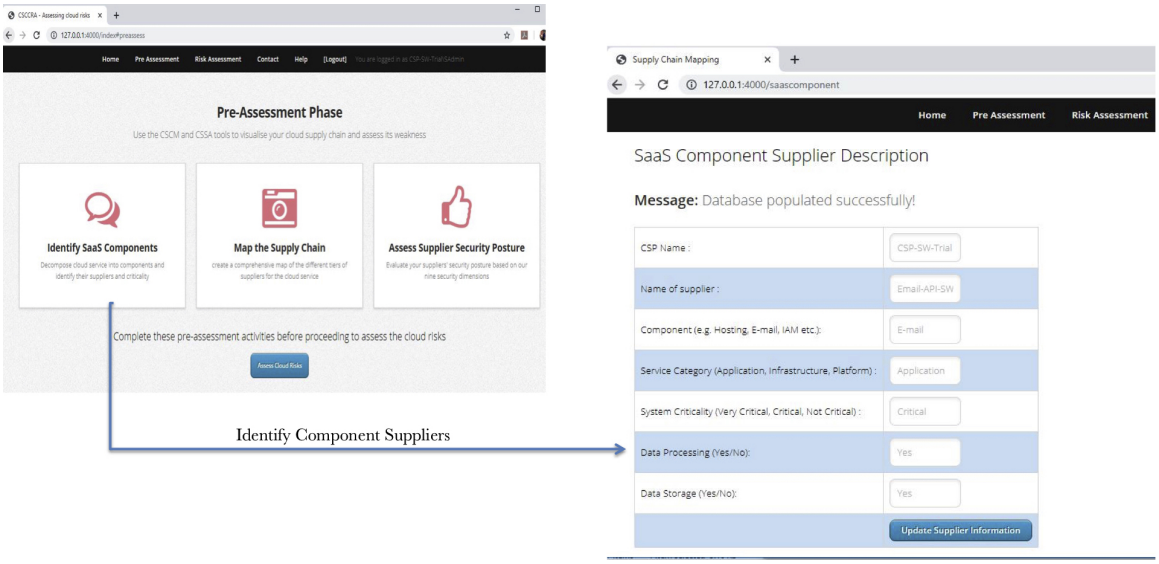
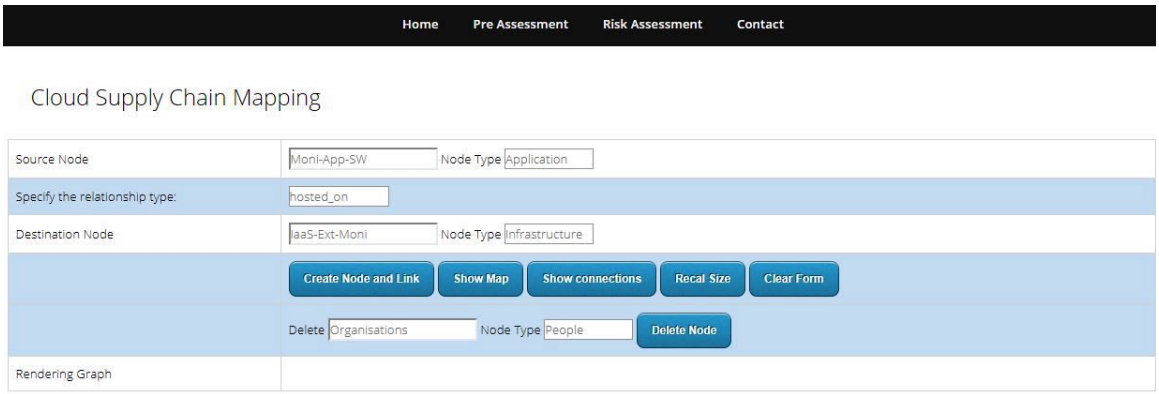


Figure E.3: CSP-SW Pre-Assessment



From	LinkType	To
Developers	modifies_data_on	CSP-SW-SaaS
Users	accesses	CSP-SW-SaaS
Moni-App-SW	monitors	CSP-SW-SaaS
CSP-SW-SaaS	hosted_on	IaaS-Pr-SW
CSP-SW-SaaS	makes_use_of	Pay-App-SW
CSP-SW-SaaS	makes_use_of	Video-API-SW

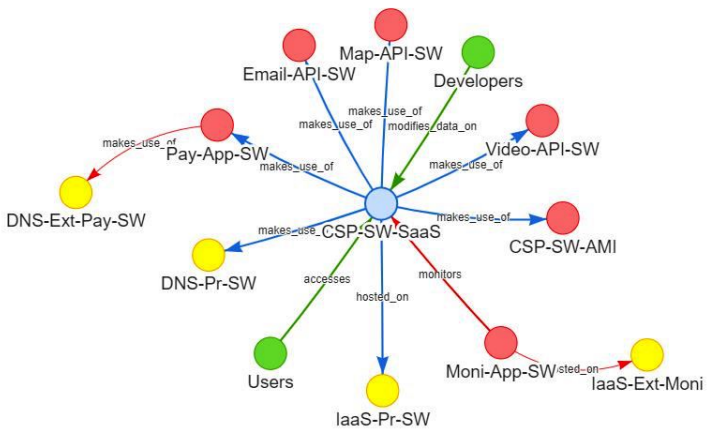


Figure E.4: CSP-SW-SaaS Supply Chain Mapping

E.3 Supplier Security Assessment

Using the information identified in the previous phases of the Pre-Assessment, i.e. SaaS Component Identification and Supply Chain Mapping, the participants proceeded to assess the security posture of the suppliers. The diagram on the left side of Figure E.5, shows how the participants rated one of the suppliers (Email-API-SW). Once they were done with rating all the suppliers, they clicked the "Show weakest link" button to confirm which of their suppliers was weak and readily susceptible to a cyber attack or those with a high risk of failure. As shown in the diagram, CSP-SW-SaaS was judged as the weakest link of the chain. The supplier assessment stage concludes the Pre-Assessment activities of the CSCCRA model. The participants had two options on how to go to the next page. Either use the Risk Assessment tab at the top of the page or scroll down to the next web page.

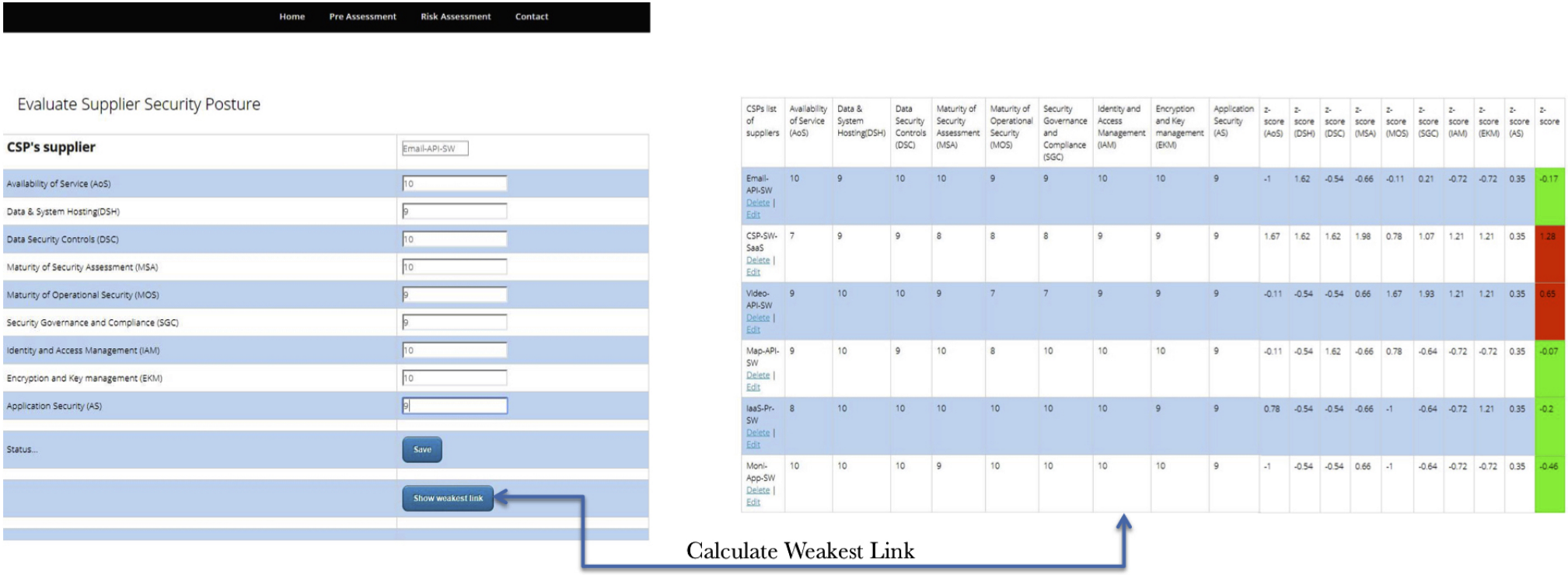


Figure E.5: CSP-SW-Trial Supplier Security Assessment

E.4 Risk Identification

On the Risk Assessment page (see Figure E.6), the participants had two main activities to complete. First was the identification of CSP risks, and the other was analysing the risks. To begin with the identification of risks, the participants clicked the "Risk Register" button, to update the risk register. Figure E.7, shows the participants entering Risk R5 after successfully saving Risk R4. Five risks were identified and stored in the risk register. Following the update of the risk register, the participants progress to the Risk Analysis page.

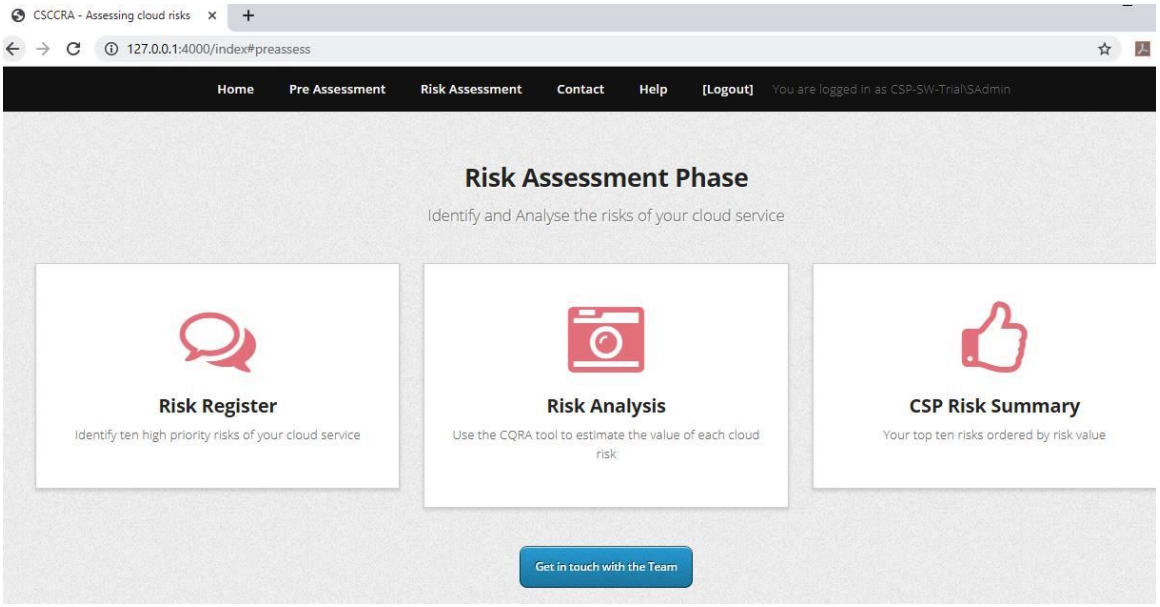


Figure E.6: Risk Assessment Page

E.5 Risk Analysis

To improve their objectivity, participants were reminded to consider the results of the pre-assessment in their estimations. Each of the three participants (Expert 1, Expert 2, Expert 3) provided an independent estimation of the probability, frequency and impact cost for each risk item. For both the probability and impact estimates, the participants provided the lower bound, most likely and upper bound estimates. For the frequency of risk event, an average value was provided. Each risk was dealt with individually, and the result of the calculation was stored in the database. Figure E.8 is a screenshot of Risk R1. For each risk calculation, once the experts have provided their estimate, the user clicks the "Calculate Risk Value" button, to arrive at the estimated risk value as shown in Figure E.8.

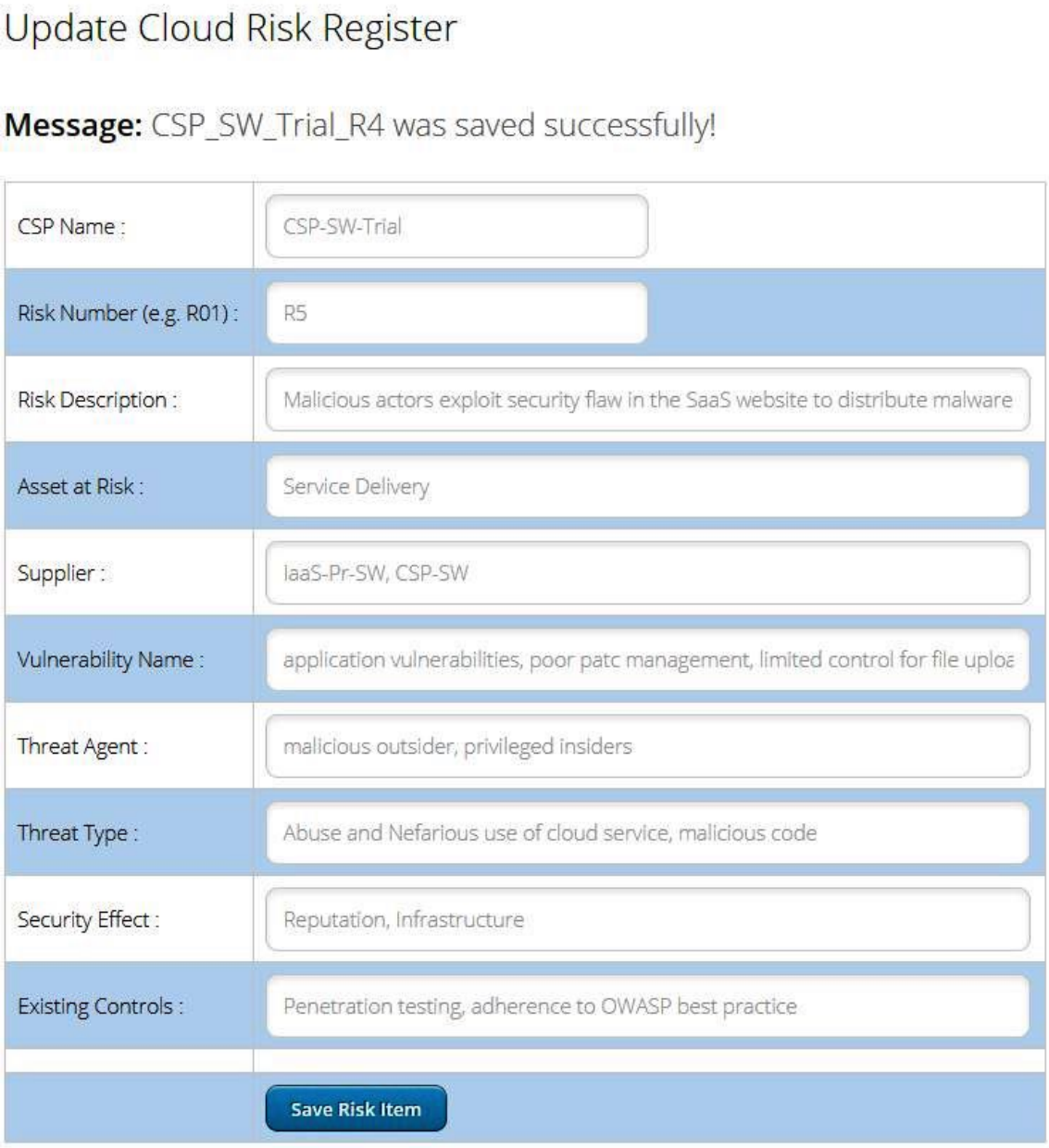


Figure E.7: Update CSP-SW-Trial Risk Register

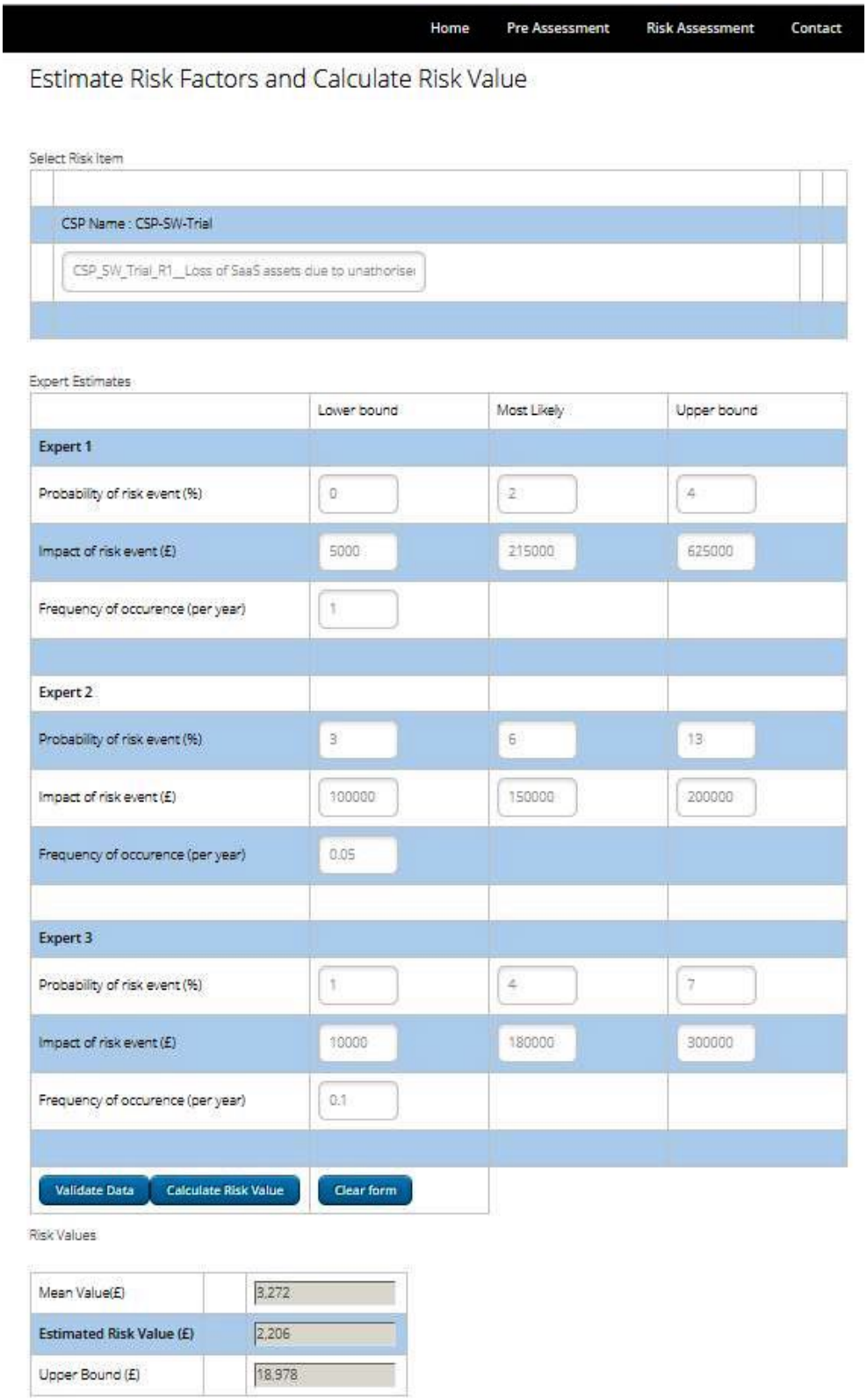


Figure E.8: CSP-SW-Trial Risk Estimation with Stakeholders

E.6 CSP Risk Summary

At the end of the risk analysis stage, the participants can click on the "CSP Risk Summary" button on the Risk Assessment page, to show an updated risk register which includes the most likely value of the risks (see Figure E.9). This stage completes the risk assessment exercise.

Refresh CSP Risk Summary

	CSP Name : CSP-SW-Trial								
Risk No	**Risk Description**	**Asset At Risk**	**Supplier**	**Vulnerability Name**	**Threat Agent**	**Threat Type**	**Security Effect**	**Existing Controls**	**Risk Value (£)**
CSP_SW_Trial_R3	Data Breach of customer PII data	Personal data, Credentials	IaaS-Pr-SW, CSP-SW	Unencrypted storage of data at rest, poor key management	malicious outsider, privileged insider, Accidental insider	Information leakage/sharing	confidentiality, privacy, reputation	existing data security policies	15091
CSP_SW_Trial_R4	Loss of SaaS application data	source code, backups, personal data	IaaS-Pr-SW	Inadequate data archiving, unencrypted storage of data at rest	provider, malicious outsider, insiders	loss due o administrative errot, ssabotage, failure of system	availability, reputation	backup restoration, offsite code repository	10570
CSP_SW_Trial_R5	Malicious actors exploit security flaw in the SaaS website to distribute malware to users	Service Delivery	IaaS-Pr-SW, CSP-SW	application vulnerabilities, poor patch management, limited control for file upload	malicious outsider, privileged insiders	Abuse and Nefarious use of cloud service, malicious code	Reputation, Infrastructure	Penetration testing, adherence to OWASP best practice	4392
CSP_SW_Trial_R1	Loss of SaaS assets due to unathorised access to hosting platform	Personal data, IP	IaaS-Pr-Sw, CSP-SW	Insufficient IAM, no encryption at rest	malicious outsider, privileged insider	sabotage, social engineering	Confidentiality, availability	Good password policy	2206
CSP_SW_Trial_R2	Unavailability of service due to DDoS	SaaS management interface	DNS-Pr-SW, IaaS-Pr-SW	Inadequate resource provisioning	malicious outsider	Denial of service	Availability	monitoring and logging	696

Figure E.9: CSP-SW Risk Summary Page

Appendix F

Sensitivity Analysis and Bounds Checking

F.1 Risk Value Calculation and Sensitivity Analysis

In this section, we present the steps taken to arrive at a risk value, followed by the sensitivity analysis of the model's output. The process will follow the steps earlier identified in Section 6.5.1, as seen below.

1. Tabulate expert risk factor estimations, combined values and risk value calculation.
2. Using spider diagrams and scenario analysis, identify the sensitivity of input variables.
3. Conduct sensitivity analysis using Scatterplots.
4. Identify important parameter(s) that influence risk value.
5. Test alternative assumptions for the value of the input risk factors.
6. Use a different risk scenario to confirm sensitivity analysis result.
7. Summarise the analysis.

Using the risk factor estimates from one of the case studies (Risk R1 from CSP-A), we will walk through the risk analysis process to determine the sensitivity of the model to variable inputs. All experiments were conducted using the Palisade @RISK tool [235].

Risk R1 - Loss of CSP-A-SaaS assets due to unauthorised access to the hosting platform (IaaS-Pro-A).

1. **Combine Experts risk factor estimates and calculate risk value**

Table F.1: Experts' Estimation of Impact, Probability and Frequency for Risk R1

Contributor	Risk Factors	Distribution	LB	ML	UB
Expert_1	Probability of risk occurrence without controls (%)	PERT	0	3	5
	Probability of risk occurrence with controls (%)	PERT	0	1	3
	Impact Cost (£)	PERT	5,000	215,000	625,000
			Average Rate		
	Frequency (/yr)	Poisson	1		
Expert_2	Probability of risk occurrence without controls (%)	PERT	5	10	25
	Probability of risk occurrence with controls (%)	PERT	1	2	8
	Impact Cost (£)	PERT	100,000	150,000	200,000
			Average Rate		
	Frequency (/yr)	Poisson	0.05		
Expert_3	Probability of risk occurrence without controls (%)	PERT	1	5	10
	Probability of risk occurrence with controls (%)	PERT	1	3	5
	Impact Cost (£)	PERT	10,000	180,000	300,000
			Average Rate		
	Frequency (/yr)	Poisson	0.1		

The lower bound, most likely and upper bound risk factor estimates of each of the experts is combined as shown below:

$$Exp_nPwCE = RiskPert(LB_n, ML_n, UB_n) \tag{F.1}$$

For example, combining Expert_3 Probability of risk occurrence estimates as shown in Table F.1, we will carry out the following:

$$Exp_3PwCE = RiskPert(10000, 180000, 300000)$$

$$Exp_nPwoCE = RiskPert(LB_n, ML_n, UB_n) \tag{F.2}$$

$$Exp_nImpact = RiskPert(LB_n, ML_n, UB_n) \tag{F.3}$$

$$Exp_nFreq = RiskPoisson(Mean) \tag{F.4}$$

Next, we generate a discrete distribution based on each expert's estimates and the weighting of their opinion (see Table F.2).

$$ComExPwCE(CPwCE) = RiskDiscrete(Exp_1PwCE : Exp_nPwCE, Exp_1Weight : Exp_nWeight) \tag{F.5}$$

$$ComExpPwoCE(CPwoCE) = RiskDiscrete(Exp_1PwoCE : Exp_nPwoCE, Exp_1Weight : Exp_nWeight) \tag{F.6}$$

$$ComExpImpact(CImpact) = RiskDiscrete(Exp_1Impact : Exp_nImpact, Exp_1Weight : Exp_nWeight) \tag{F.7}$$

Table F.2: Combined Expert Estimation of Risk R1 after five simulations of 100,000 iterations each

Combined Expert Risk Factor Estimates			
Risk Factors	**LB**	**ML**	**UB**
Probability of risk occurrence without controls (%)	1.70	6.70	16.00
Probability of risk with controls (%)	0.50	2.20	4.40
Impact Cost (£)	91,852	192,996	391,144
Frequency (/yr)	0.10		

$$ComExpFreq(CFreq) = RiskDiscrete(Exp_1Freq : Exp_nFreq, Exp_1Weight : Exp_nWeight) \tag{F.8}$$

Table F.3: CSP-A Expert Opinion Weightings

Contributor	**Weight**	**Sample**
Expert_1	4	0.4
Expert_2	3	0.3
Expert_3	3	0.3
Total	**10**	**1**

$$ERV\_WC = CImpact * CFreq * CPwCE \tag{F.9}$$

$$ERV\_WoC = CImpact * CFreq * CPwoCE \tag{F.10}$$

By applying equations E.9 & E.10, the risk assessor is then able to calculate the risk value for when controls are in place and otherwise (see Table F.4). The final risk value is presented in monetary terms (£) with three estimates (lower bound, the mean value and upper bound). Although, when we consider the threat and vulnerability of the application combined with our understanding of CSP processes, we arrive at a Most Likely (ML) risk value which sits around the 85% percentile of the ERV_WoC distribution.

Table F.4: Estimated Risk Value based on Combined Expert Estimates

Output (Estimated Risk Value)	**Without Controls (ERV_WoC)**	**With Controls (ERV_WC)**
5% Percentile (£)	0.00	0.00
Mean (£)	5,772	1,910
95% Percentile (£)	31,293	10,144
Estimated Risk Value (Most Likely)	**£4,610**	

2. **Using Spider Diagrams and Scenario Analysis, identify the sensitivity of Input variables.**

   We begin the analysis of our SA result by presenting the change in the objective function value (risk value) for the different parameter values (risk factors). Here we make use of a spider diagram because it enables us to compare the impact of various parameters on the objective function while presenting the result on a single graph. Figure F.1 shows how the mean risk value changes as each input vary through its percentiles.

   The diagram shows that, of the three risk factors, the frequency of risk occurrence (freq) has the most significant effect on the mean risk value. While the impact and probability risk factors had a steady influence on the risk value, the frequency risk factor had the steep rise from the 68^{th} percentile and is considered the most influential factor for risk values ranging from £4,000 to £12,000. However, one must bear in mind that the Experts' estimation of the frequency of risk event ranged from 0.05 to 1, and it would seem that it is only as the value approaches the higher estimation that frequency begins to impact risk value. This observation is in line with that of Pannell [236], where he observed that where the parameter is small, percentage changes may be substantial relative to those of other variables.

   Following the above observation with scenario analysis, where we identify which of the uncertain inputs within a selected percentile was significantly different from its value in the rest of the iterations. Figures F.2 & F.3 shows the possible effects of the risk factors on the dependent variable, i.e. risk value. When the scenario analysis was conducted for input variables at 50% percentile of the risk value, none of the input variables was judged to be significantly different from the rest of the iteration. That said, at the 75% percentile mark, the frequency input variable made a significant difference in the risk value output. As shown in Figure F.2, the median of the frequency input variable (M2) where risk output is greater than 75%, was 1.24 standard deviations from the median of the rest of the iterations (M1) and falls within 90% of the input distribution.

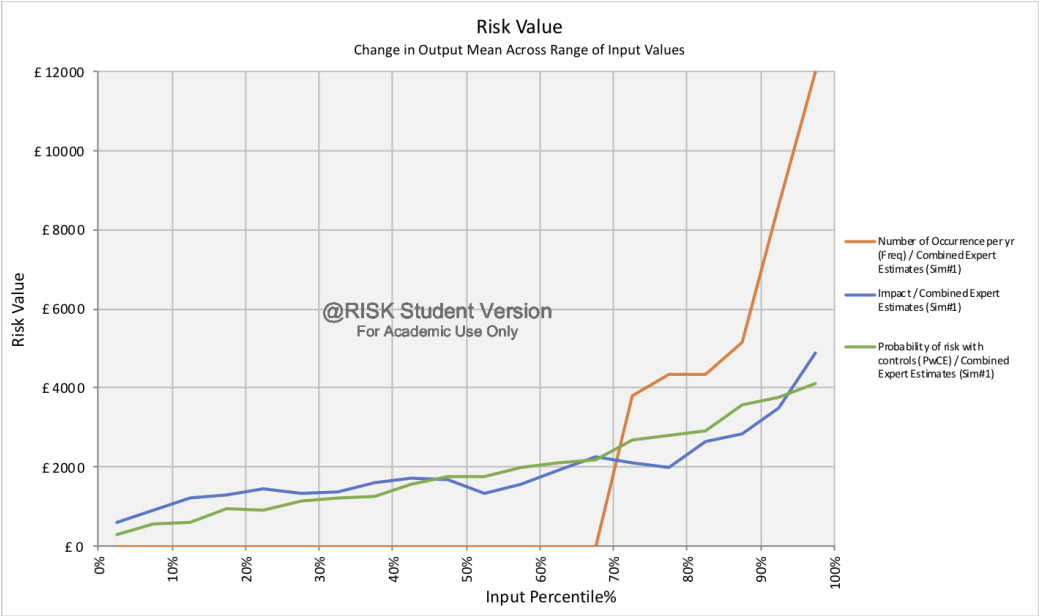


Figure F.1: The impact of risk factor inputs on risk value output

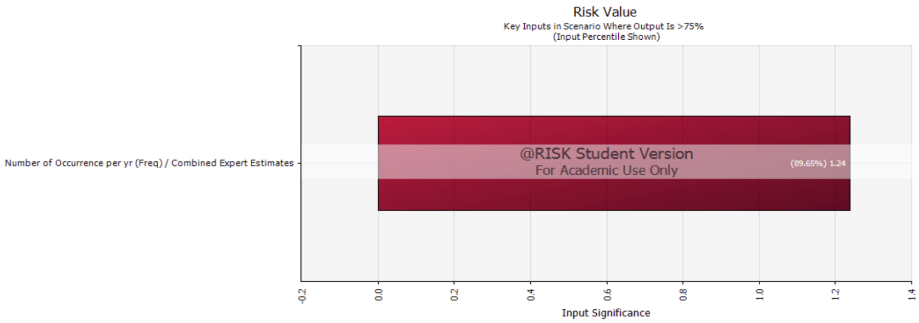


Figure F.2: Key inputs in scenario where risk value is greater than 75%

Furthermore, conducting the same scenario analysis to identify key inputs in scenarios where the risk output is greater than the 90% percentile of risk values, both the probability and frequency input variables were significant. Figure F.3 shows that the median for the frequency input was 2.48 standard deviations from the median of the rest of the iterations, while that of probability input variable was only 0.85 standard deviation away. At the calculation of key inputs contributing to the 95^{th} percentile of the risk value, all input variables were significant, but the frequency risk factor had the dominant influence.

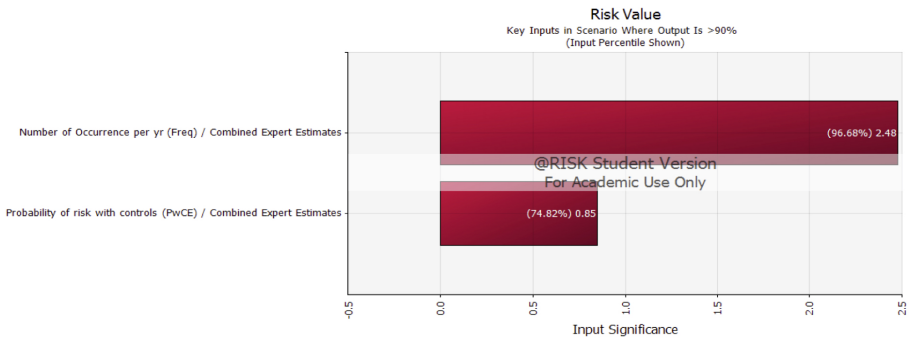


Figure F.3: Key inputs in scenario where risk value is greater than 90%

3. **Sensitivity Analysis using Scatterplots.**

   Here, we use the sample of the model input and output to produce a scatterplot. We use the scatterplot to investigate the behaviour of the CSCCRA model, and to determine which risk factor has the most significant influence on the estimated risk value (output). We begin the analysis with the probability of risk occurrence, followed by the impact value of the risk and frequency. For each of the factors, the @RISK tool also calculates both the Pearson and Spearman rank correlation coefficients.

   Figure F.4 shows a scatterplot of the values of the probability (independent variable) against that of the risk value (dependent variable). Here we see that although it looks like a relationship exists between the two variables, it is somewhat random, going by the correlation coefficients. The Pearson correlation coefficient for the relationship between probability and risk value is calculated to have a value of 0.2380, while the Spearman's rank correlation coefficient is 0.0930.

   Also, Figure F.5 shows a scatterplot of the risk value *(y-axis)* against the impact value *(x-axis)*. This plot, somewhat similar to the previous, confirms a weak relation-

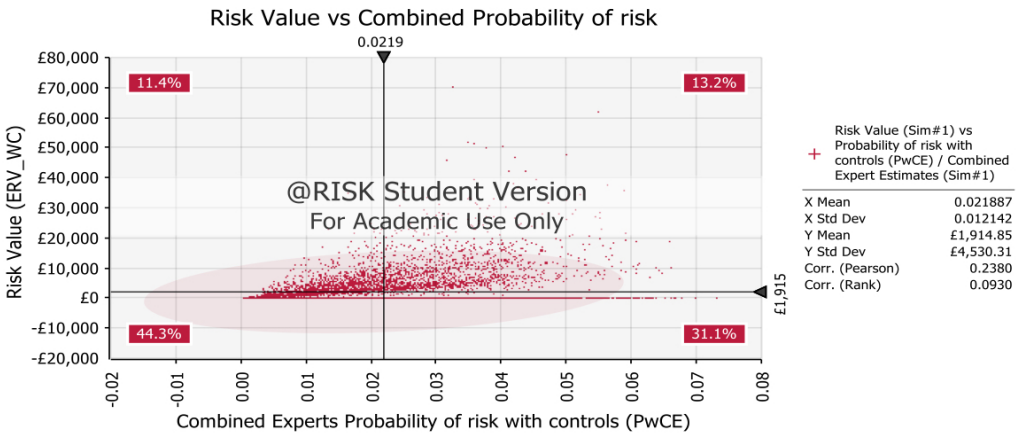


Figure F.4: Scatterplot of Risk value versus Probability of risk event

ship between the variables. The Pearson correlation coefficient for the relationship is 0.2042, while the Spearman's rank correlation coefficient is 0.0648.

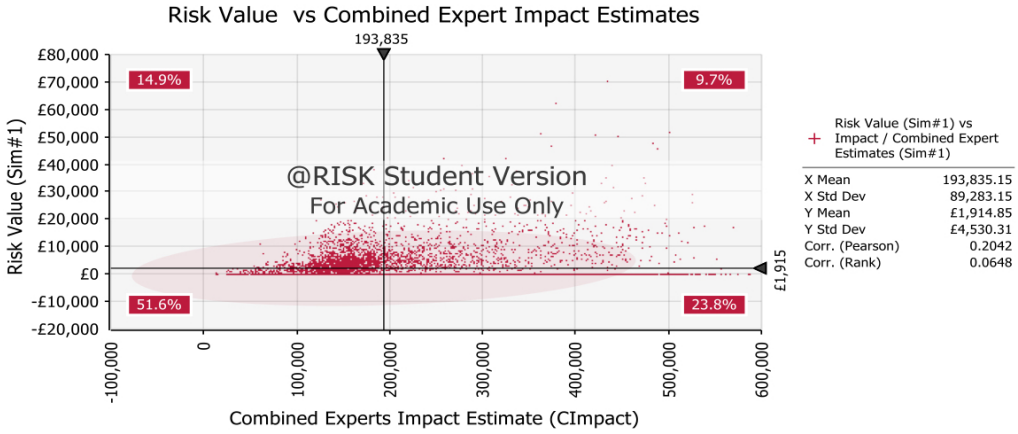


Figure F.5: Scatterplot of Risk value versus Impact of risk event

Lastly, Figure F.6 shows a scatterplot of the risk value against the frequency of risk occurrence. This scatter plot differs from the previous two, in that its strength and the direction of the relationship is positive. The plot confirms a linear and monotonic relationship between the variables is strong [206]. The Pearson correlation coefficient for the relationship is calculated to be 0.7641, while the Spearman's rank correlation coefficient is almost perfect with a value of 0.9821.

The results show that the monotonic relationship of the impact and probability variables against the risk value is weak, hence the low score in the Spearman correlation coefficient. Although all input variables have a varying range of linear relationship with the risk value output, the frequency risk factor has the strongest positive linear relationship. Overall, the scatterplots show that the risk value (output) is more sen-

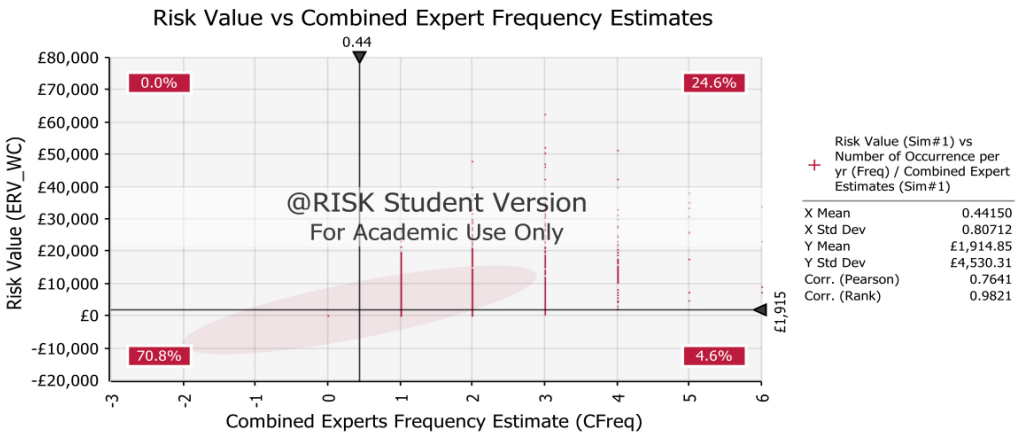


Figure F.6: Scatterplot of Risk value versus Frequency of risk event

sitive to frequency than it is to impact, and the ordering of the input factors by their influence on the risk value is

$$\textbf{Frequency} > \textbf{Impact} > \textbf{Probability} \tag{F.11}$$

4. **Test alternative assumptions for the value of the input risk factors**

   To further test the robustness of the results of the model in the presence of uncertainty and increase our understanding of the relationship that exists between the input risk factors and output risk value, we make changes to the Experts' estimations. We raise the values of one risk factor, leaving the others in their original state, and show how the mean risk value changes with this new input using a spider diagram.

   Scenario I: Increase Impact value

   Table F.5 shows the changed impact value estimates in bold while Figure F.7 shows the resulting spider diagram for the risk value calculation. As seen in Figure F.7, the increase in impact values made no distinct change to the original spider diagram shown in Figure F.1, except for the increase in risk value. The frequency risk factor remains the dominant risk factor that influences the risk value. Also, we see that the change in impact value also reduces the influence of the impact risk factor on the overall risk value, particularly after the 60^{th} percentile.

Table F.5: Modified Experts' Estimation of Impact; Probability and Frequency unchanged

Contributor	Risk Factors	Distribution	LB	ML	UB
Expert_1	Probability of risk occurrence with controls (%)	PERT	0	1	3
	Impact Cost (£)	PERT	**300,000**	**700,000**	**1,000,000**
	Frequency (/yr)	Poisson	1		
Expert_2	Probability of risk occurrence with controls (%)	PERT	1	2	8
	Impact Cost (£)	PERT	**350,000**	**580,000**	**900,000**
	Frequency (/yr)	Poisson	0.05		
Expert_3	Probability of risk occurrence with controls (%)	PERT	1	3	5
	Impact Cost (£)	PERT	**210,000**	**400,000**	**750,000**
	Frequency (/yr)	Poisson	0.1		

   Scenario II: Return Impact value to original& increase Probability estimate

   In this 2^{nd} scenario, we default the Impact values to the original Expert estimates and increase the probability estimates (see Table F.6). As shown in Figure F.8, raising the probability estimates did not make a significant change in the factors that influenced the risk value based on input percentile. While the rise in probability increased the estimated value of risk (as expected), it did not increase the influence of the risk factor, but reduced it, making it the least influential factor in the risk calculation.

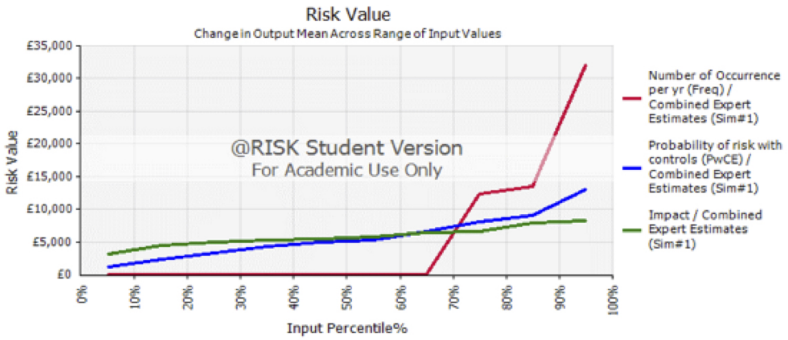


Figure F.7: Spider diagram illustrating a change in impact values

Table F.6: Modified Experts' Estimation of Probability; Impact and Frequency unchanged

Contributor	Risk Factors	Distribution	LB	ML	UB
Expert_1	Probability of risk occurrence with controls (%)	PERT	**10**	**20**	**30**
	Impact Cost (£)	PERT	5,000	215,000	625,000
	Frequency (/yr)	Poisson	1		
Expert_2	Probability of risk occurrence with controls (%)	PERT	**12**	**25**	**40**
	Impact Cost (£)	PERT	100,000	150,000	200,000
	Frequency (/yr)	Poisson	0.05		
Expert_3	Probability of risk occurrence with controls (%)	PERT	**6**	**14**	**20**
	Impact Cost (£)	PERT	10,000	180,000	300,000
	Frequency (/yr)	Poisson	0.1		

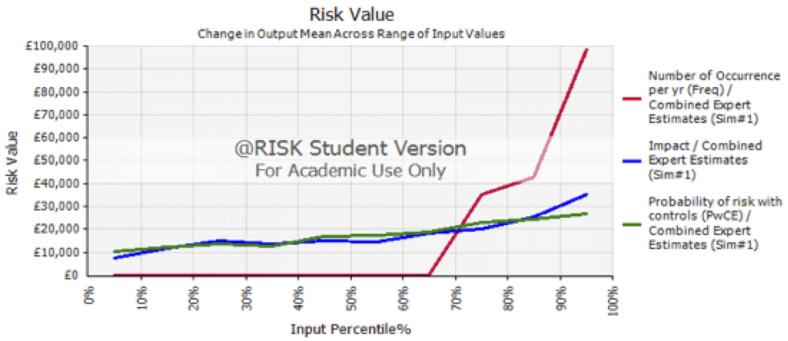


Figure F.8: Spider diagram illustrating a change in probability values

Scenario III: Return Probability value to original & increase Frequency estimate

In this scenario, we default the probability values to the original Expert estimates and increase the frequency estimates (see Table F.7).

So far, the SA has shown the frequency of risk event as an important risk factor that has a significant impact on the model's performance. Although, in the course of our analysis, we acknowledged that this influence might be as a result of the reduced range of the frequency estimates (initially between 0.05 to 1 event per year). Therefore, in this scenario, we increased the range of frequency to between one (1) and three (3) events per year. The result of this change is depicted in Figure F.9.

As shown in Figure F.9, by increasing the frequency estimate, the influence of the frequency risk factor reduced while the other factors also increased in importance, particularly when compared to the original spider diagram generated from the Experts' estimate (see Figure F.1). To illustrate the sensitivity of the model to this change in the frequency factor, we calculated the Pearson and Spearman rank correlation coefficients and presented the result in a scatter plot (see Figure F.10).

While the result of this calculation maintains the superiority of the frequency risk factor, it also supports the claims of Pannell [236], where he states that where the parameter is small, percentage changes may be substantial relative to those of other variables. As shown in the scatter plot, where the range of an input variable (frequency) is comparable to other variables, the distinction between their importance will in some cases, be minimal.

Table F.7: Modified Experts' Estimation of Frequency; Impact and Probability unchanged

Contributor	Risk Factors	Distribution	LB	ML	UB
Expert_1	Probability of risk occurrence with controls (%)	PERT	0	1	3
	Impact Cost (£)	PERT	5,000	215,000	625,000
	Frequency (/yr)	Poisson	**3**		
Expert_2	Probability of risk occurrence with controls (%)	PERT	1	2	8
	Impact Cost (£)	PERT	100,000	150,000	200,000
	Frequency (/yr)	Poisson	**1.5**		
Expert_3	Probability of risk occurrence with controls (%)	PERT	1	3	5
	Impact Cost (£)	PERT	10,000	180,000	300,000
	Frequency (/yr)	Poisson	**1**		

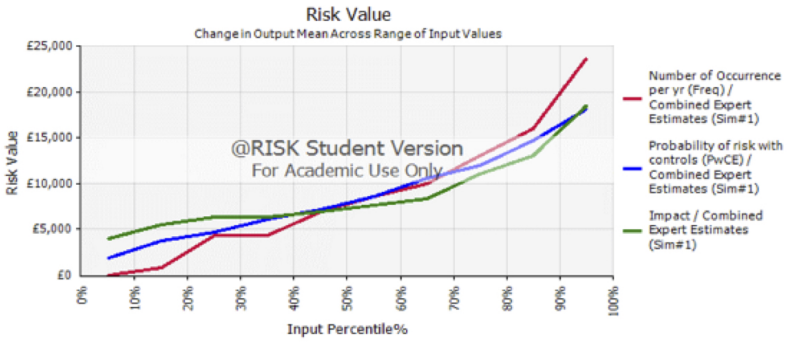
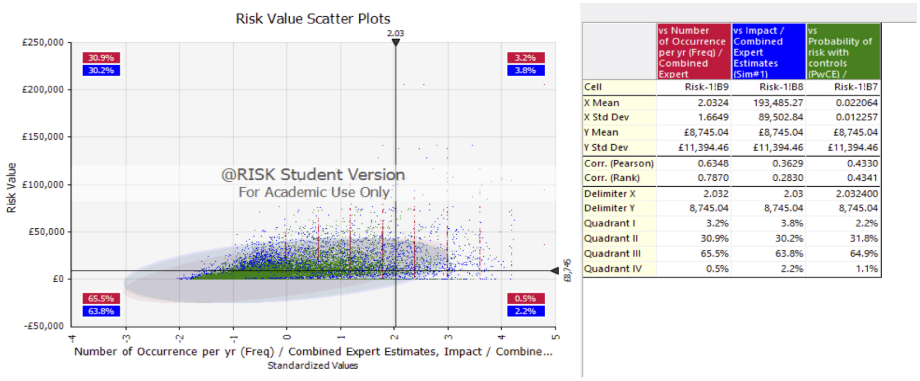


Figure F.9: Spider diagram illustrating a change in frequency values



	vs Number of Occurrence per yr (Freq) / Combined Expert	vs Impact / Combined Expert Estimates (Sim#1)	vs Probability of risk with controls (PwCE) /
Cell	Risk-1!B9	Risk-1!B8	Risk-1!B7
X Mean	2.0324	193,485.27	0.022064
X Std Dev	1.6649	89,502.84	0.012257
Y Mean	£8,745.04	£8,745.04	£8,745.04
Y Std Dev	£11,394.46	£11,394.46	£11,394.46
Corr. (Pearson)	0.6348	0.3629	0.4330
Corr. (Rank)	0.7870	0.2830	0.4341
Delimiter X	2.032	2.03	2.032400
Delimiter Y	8,745.04	8,745.04	8,745.04
Quadrant I	3.2%	3.8%	2.2%
Quadrant II	30.9%	30.2%	31.8%
Quadrant III	65.5%	63.8%	64.9%
Quadrant IV	0.5%	2.2%	1.1%

Figure F.10: Scatter plot showing the relationship of risk factors after frequency value change

5. **Use a different risk scenario to confirm sensitivity analysis result**

   Having gone through steps 1 to 4 and confirmed the influence of the frequency of risk occurrence variable on the estimated value of risk, we considered using another risk scenario to validate our observations. To do that, we looked through all the risk items to find a cloud risk scenario where all expert estimations are somewhat close, and there are no small parameters. We adopted this approach to investigate the influence of the frequency variable in situations where the spectrum of input variables where comparable. We identified Risk R7 from the first case study (CSP-A) and using the @RISK tool, we calculated the correlation coefficients for the input variables, presenting the result in scatter plots and spider diagrams.

   Risk R7 - Unavailability of service for 6 hours due to software code bug (CSP-A).

   It can be seen from the data in Table F.8, that the LB, ML and & UB expert estimates of the input variables are comparable. This might be because the CSP is aware of the risk scenario and its potential cost. The risk value was estimated as £875, and as

Table F.8: Experts' Estimation of Impact, Probability and Frequency for Risk R7

Contributor	Risk Factors	Distribution	LB	ML	UB
Expert_1	Probability of risk occurrence with controls (%)	PERT	5	10	15
	Impact Cost (£)	PERT	2,000	3,000	5,000
	Frequency (/yr)	Poisson	2		
Expert_2	Probability of risk occurrence with controls (%)	PERT	2	8	14
	Impact Cost (£)	PERT	500	1,000	10,000
	Frequency (/yr)	Poisson	0.75		
Expert_3	Probability of risk occurrence with controls (%)	PERT	5	15	20
	Impact Cost (£)	PERT	1,500	5,000	12,000
	Frequency (/yr)	Poisson	1		

shown in Figure F.11, all the input variables influenced the risk output. Here again, the frequency input variable contributed the most to the change in output mean across the different percentiles, making it the most influential risk factor. Likewise, as seen in Figure F.12, the relative sensitivity of the risk value output to frequency is higher than the other two input variables. Where the Spearman's rank correlation coefficients for the frequency variable was **0.8824**, the impact variable had a value of **0.2936**, while probability had a low score of **0.1852**.

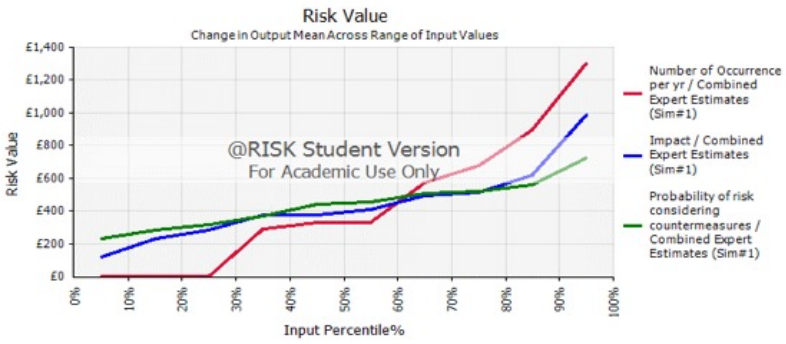


Figure F.11: Spider diagram of Risk R7

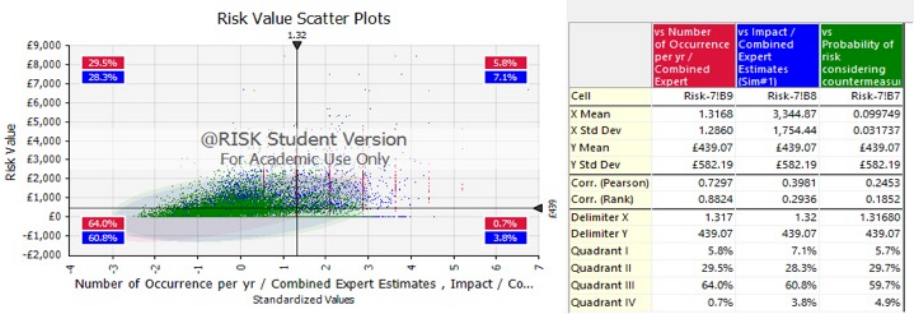


Figure F.12: Scatter plot of the Input variables with their correlation coefficients

Overall, and in a similar fashion to Risk R1, the scatter plot for Risk R7 shows that the Risk value (output) is most sensitive to frequency, followed by impact and

probability. Therefore, a safe order for the sensitivity analysis of the input variables of the CSCCRA model in its calculation of cloud risk value is as shown below:

$$\textbf{Frequency} > \textbf{Impact} > \textbf{Probability} \tag{F.12}$$

6. **Summarise the analysis.**

In this section, we conducted an experiment to show how the uncertainty in the risk value output of the CSCCRA model can be attributed to the different input variables. We conducted multiple iterations of the risk calculation, changing the value of the parameters in a bid to identify the crucial factors. We determined the frequency variable as the most influential risk factor, with a significant impact on the model's performance. In our analysis, we assumed the independence of the three risk factors, since they are based on experts judgement of the risk scenario.

While the sensitivity analysis study provided us with a good view of the capability of the model to evaluate cloud risk, we sought to determine if the difference in the statistical distribution of the factors is relevant to the influence they exhibit. While the implementation of the CSCCRA model adapted the frequency variable as a Poison distribution, it used the PERT distribution for the impact value and probability variables. A likely but unconfirmed reason for the influence of the frequency variable might be the difference between discrete and continuous distributions. The discrete nature of the Poison distribution, where the correlation of the mean & standard deviation is based on independent occurrences and often limited to a small range, would seem to have made a difference in the risk calculation. However, seeing that the frequency variable expresses the probability of a given number of independent events occurring within a fixed time, we maintain the need to adopt the best distribution for such a situation, i.e. Poisson distribution.

Lastly, based on the result of this analysis, one can suggest that the optimal strategy for estimating risk value using the CSCCRA is to ensure that Expert's estimation of the frequency of risk occurrence is objective, defensible and fact-based. This best-bet strategy will ensure the estimated risk value will not be skewed in the direction of the experts' subjectivity (over or under), but will be realistic.

In conclusion, this sensitivity analysis found no apparent errors in the CSCCRA model, validated the robustness of the model for cloud risk value estimations and established the degree to which the model was sensitive to its input variables.

F.2 Bounds Checking

In complying with best practice, we conducted a bounds check on the CQRA tool to make sure all user inputs are of the expected type and range.

Using the domain attributes of each variable (risk factor), we specify its type and range of possible values. A domain can be various combinations of continuous or discrete and bounded or unbounded [193]. Each risk factor (probability, impact, frequency) presents a different challenge with regards to bounds checking and as such, we implemented a combination of attributes to ensure consistency of risk value results in the face of extreme or irrational inputs. However, due to the limitations in the Microsoft Excel program, which our @Risk simulation tool integrates with, our validation criteria only checked for a single data type and value range. For instance, we could not validate that the user input for the probability of risk with controls is lower than or equal to the probability of risk without controls. Table F.9 shows the domain attributes for each risk factor, including the bounds check to constrain the variable within lower and upper limits.

Our validity test involves displaying a message to the end-user in situations where an invalid input has been entered. Figures E.13 to E.16 presents four scenarios where the user entered invalid or out of range values for the different risk factors. The "stop" error message presents the user with the valid range for the input, and request them to revise their data before proceeding with the rest of the estimations.

Table F.9: Criteria for conducting Input Validation and Bounds Checking

Input Validation and Bounds Checking			
Risk Factors	**Lower Bound**	**Most Likely**	**Upper Bound**
Probability without Controls (PwoCE)	PwoCE_LB is a decimal value between 0 & 100	PwoCE_ML is a decimal value between 0 & 100 PwoCE_LB <= PwoCE_ML <= PwoCE_UB	PwoCE_UB <=100 PwoCE_UB >= PwoCE_ML
Probability with Controls (PwCE)	PwCE_LB is a decimal value between 0 & 100	PwCE_ML is a decimal value between 0 & 100 PwCE_LB <= PwCE_ML <= PwCE_UB	PwCE_UB <= 100 PwCE_UB >= PwCE_ML
Impact Cost	Impact_LB is a whole number	Impact_ML is a whole number Impact_LB <= Impact_ML <= Impact_UB	Impact_UB >= Impact_ML
Frequency of risk event (Freq)	Freq is a decimal value between 0 & 365 (i.e. 1 event per day)		

Scenario 1: End-user enters an out-of-range value for PwoCE_LB.

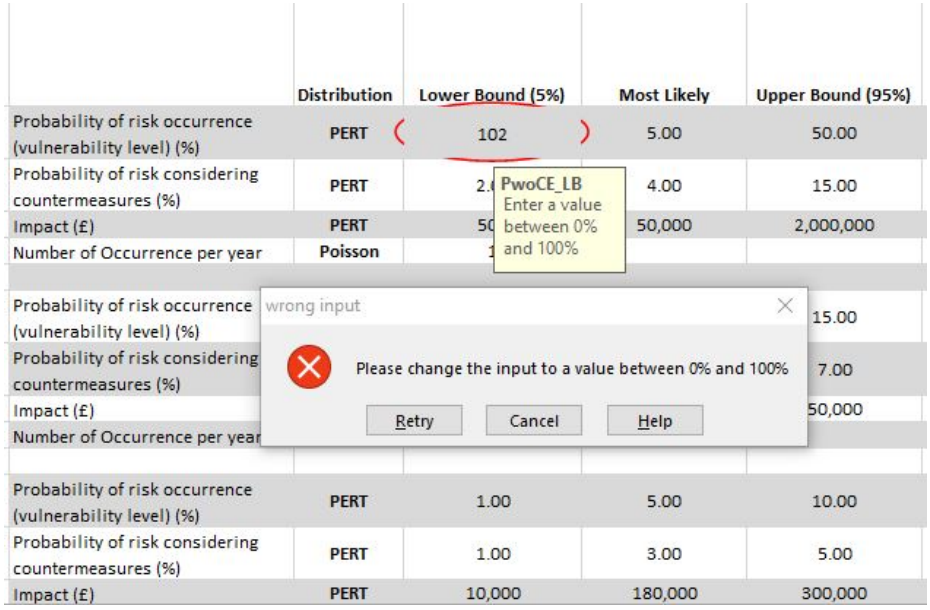


Figure F.13: Invalid input for PwoCE_LB

Scenario 2: End-user enters a value for PwCE_ML, which is higher than the upper bound estimate (PwCE_UB).

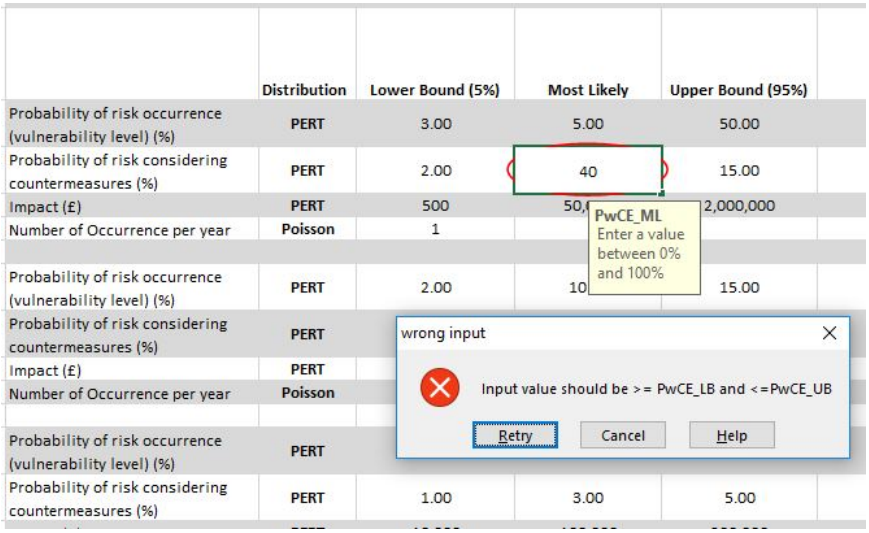


Figure F.14: Invalid input for PwCE_ML

Scenario 3: End-user enters a value for Impact_UB, which is lower than the most likely estimate (Impact_ML).

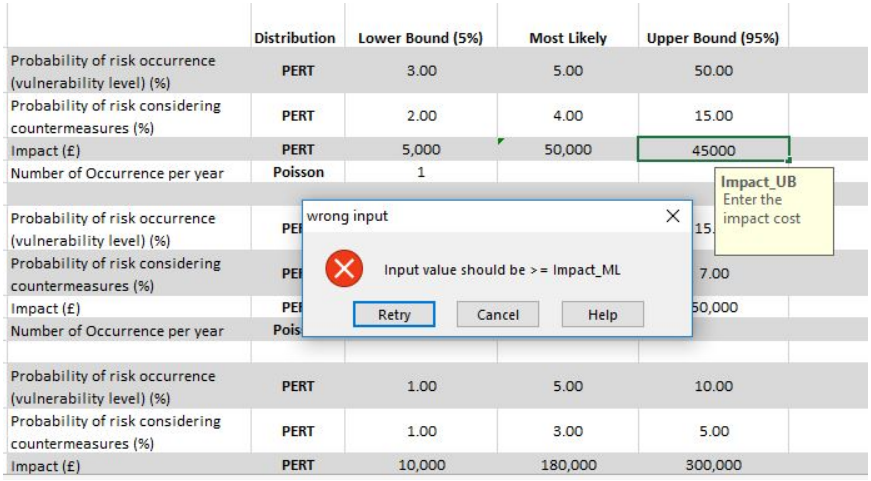


Figure F.15: Invalid input for Impact_UB

Scenario 4: End-user enters an out-of-range value for Frequency of risk occurrence. The rate of occurrence has been limited to between 0 and 365. In this instance, the user enters a value of -1.

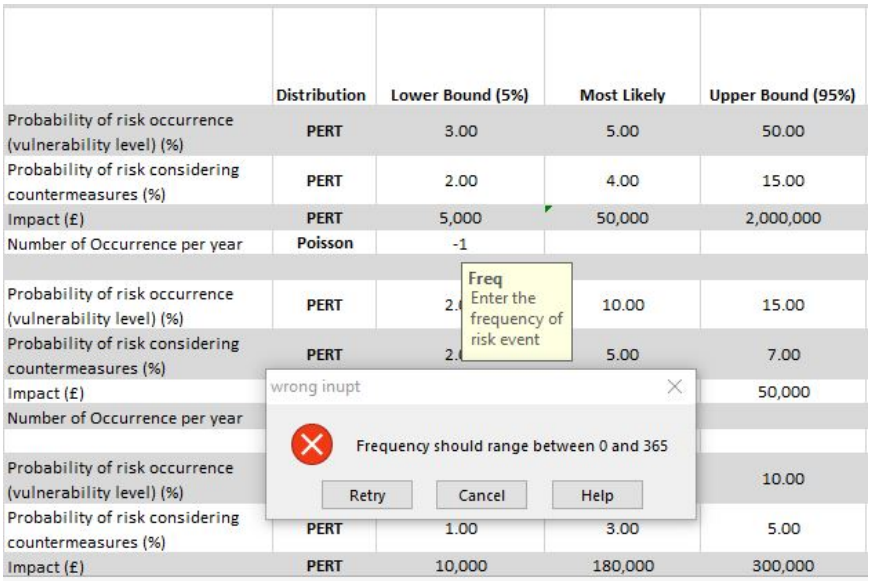


Figure F.16: Invalid input for Frequency