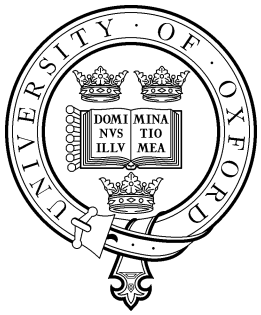
Foundations for A Trustworthy Data Security Level Agreement Capability Framework

An Indonesian Government Case Study



Yudhistira Nugraha

Linacre College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Michaelmas 2017

Foundations for A Trustworthy Data Security Level Agreement Capability Framework

D.Phil. Thesis

Yudhistira Nugraha

Linacre College

Abstract

After the publication of secret documents by a former U.S. NSA contractor Edward Snowden, many governments around the world have been hesitant to procure external information system services provided by global cloud service providers, such as Amazon Web Services, Microsoft, and Google Cloud. There is a growing concern about preserving the confidentiality of sensitive data across government agencies when using such external services. The use of certification schemes is becoming more critical to assure the security of services offered. This situation is problematic because many certification schemes aim to demonstrate compliance with a security standard, rather than achieve a specified level of security. Despite the benefits of security certification schemes like Common Criteria (CC), an assurance-based certification process does not scale well to service provision.

This thesis aims to investigate the concept of system assurance and trustworthiness in service provisioning, especially when government agencies procure external information system services to support the delivery of public services. By using work on the Indonesian Government's data confidentiality requirements, this thesis develops principles as foundations for *a trustworthy data security level agreement (TDSLA) capability framework* as a new assurance mechanism for service provisioning based on discrete levels of security assurance incorporated into the formulation of a service level agreement (SLA). The principles which have emerged from the empirical qualitative data collection were evaluated and validated using three approaches, namely: 1) reflection against related work; 2) testimonial validity through participants' feedback; and 3) application of transferability using cases from Amazon Web Services -UK Government Cloud (AWS G-Cloud) and the US Federal Risk and Authorization Management Program (AWS FedRAMP).

The thesis claims three contributions (methodological, empirical and conceptual) towards the stated research question and sub-research questions. The first contribution is developing and conducting an adaptive Wideband Delphi method to engage with elite participants as well as minimise barriers to completing data collection activities. An additional methodological contribution is the application of grounded theory to the Delphi study results as a means of providing a theoretical understanding of the specific categories as components of principles and framework. The second contribution is developing a foundation for future research by providing various understandings of government security needs, government SLA data confidentiality requirements, and service provision for data confidentiality in SLAs. The third contribution is developing and validating principles as foundations for a TDSLA capability framework. The key inspiration for building the proposed framework is the CC certification process. The CC aims to certify levels of security for products while the TDSLA capability framework aims to certify levels of security for services.

Publications

The following publications have resulted from this research. Professor Andrew Martin and Professor Ian Brown are listed as co-authors on various publications in recognition of their supervisory roles in this research. I am the sole author of any text from these publications that have been used in this thesis.

Journal Papers

- Y. Nugraha, I. Brown and A. S. Sastrosubroto. "An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements". In: *IEEE Transactions on Emerging Topics in Computing*. vol. 4. no. 1. pp. 47-59. 2016.
- Y. Nugraha and A. Martin. Understanding Government Service Level Agreement Confidentiality Requirements: An Indonesian Government Case Study. This manuscript is in the process of submission to a journal publication.
- Y. Nugraha and A. Martin. A Study Investigating Service Provision for Data Confidentiality in Service Level Agreements: An Indonesian Government Case Study. This manuscript is in the process of submission to a journal publication.
- Y. Nugraha and A. Martin. Principles for a Trustworthy Data Security Level Agreement Capability Framework: An Indonesian Government Case Study. This manuscript is in the process of submission to a journal publication.

Conference and Workshop Papers

- Y. Nugraha and A. Martin. Investigating SLA Confidentiality Requirements: A Holistic Perspective from the Government Agencies. In Proceedings 11th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2017), pp. 154-160, IARIA, 2017.
- Y. Nugraha and A. Martin. Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments. In: Steghöfer JP., Esfandiari B. (eds) Trust Management XI. IFIPTM 2017. IFIP Advances in Information and Communication Technology, vol 505, pp.57-75, Springer, Cham, 2017.
- Y. Nugraha and A. Martin. Towards the Classification of Confidentiality Capabilities in Trustworthy Service Level Agreements. In Proceedings 5th International Conference on Cloud Engineering (IC2E 2017), pp. 304-310, IEEE, 2017.
- Y. Nugraha and A. Martin. Understanding Trustworthy Service Level Agreements. In Proceedings IFIP WG 11.4 International Workshop on Open Research Problems in Network Security (iNetSec), Springer, 2017.
- Y. Nugraha and A. Martin. Trustworthy Service Level Agreements: An Approach for Protecting Government Data Secrecy. Work in Progress. In 10th Layered Assurance Workshop, Annual Computer Security Applications Conference (ACSAC), 2016.

- Y. Nugraha. Security Assurance Requirements Engineering (STARE) for Trustworthy Service Level Agreements. In Proceedings 23rd International Conference on Requirements Engineering (RE'15), pp. 398-399, IEEE, 2015.

Other Publications not Related to this Thesis

- Y. Nugraha, I. Brown, T. Roberts, A.S. Sastrosubroto. The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford Internet Institute, University of Oxford, 2016.
- Y. Nugraha, K.Kautsarina and A.S. Sastrosubroto. Towards data sovereignty in cyberspace. In Proceedings 3rd International Conference on Information and Communication Technology (ICoICT), pp. 465-471, IEEE, 2015.

Invited Talks

- Y. Nugraha. Global Trends in Cybersecurity Threats and Attacks. *Security Awareness Program for Executive Leaders*, Ministry of Communications and Information Technology, Depok, 6 September 2017.
- Y. Nugraha. The Use of Cyberspace for Terrorism in Indonesia. *Focus Group Discussion*, State Intelligence Agency, Jakarta, 11 September 2017.
- Y. Nugraha. Design and Implementation of National Cybersecurity Strategies. *The Future of Cybersecurity Capacity in Indonesia*, Jakarta, 28 March 2016.
- Y. Nugraha. Research Challenges in Cybersecurity. Guest Lecture Series, University of Indonesia, Jakarta, 30 August 2016.
- Y. Nugraha. Towards Data Sovereignty in Indonesia. *International Indonesian Scholars Association*, Online Lecture, 31 May 2015.
- Y. Nugraha. An Adaptive Wideband Delphi Method to Study State Cyber-Defense Requirments. *Academic Forum and Networking Exchange - PPI Oxcford - Cambridge*, St. John College, University of Cambridge, 22 March 2015.

Acknowledgements

All Praise is due to Allah, the Lord of the whole world for giving me the courage, strength and enthusiasm to complete this thesis.

First of all, I would like to thank my supervisor, Professor Andrew Martin, for his insight, support and guidance throughout my DPhil. I also appreciate the time he dedicated to reading chapter by chapter of the draft thesis. I would like to extend my appreciation to my co-supervisor, Professor Ian Brown, for two-year supervision (2014 - 2016) and his first guidance to prepare this research. I was grateful for all the opportunities to work with the Oxford Internet Institute.

I would also like to thank my internal and external examiners, Professor Ivan Flechais and Dr Jat Singh (University of Cambridge) for their helpful and constructive feedback and comments. I also appreciate the valuable advice and input of my assessors (Prof Jirotka, Prof Flechais and Prof Simpson) on this work as it progressed during my transfer and confirmation of status.

I thank my master's supervisor, Dr William Tibben at the University of Wollongong - Australia, for laying the foundations for this research endeavour, especially for introducing research methods. I also thank you for the feedback and comments on some draft chapters of this thesis.

My greatest thanks to Indonesian senior officials of the Ministry of Communications and Information Technology (KOMINFO), Dr Cahyana Ahmadjayadi, Dr Ashwin Sasongko Subroto, Pak Bambang Heru, Pak Semmy, Dr Basuki Yusuf Iskandar, Pak Djoko Agung, Ibu Mariam, Pak Aidil, Pak Riki, Pak Pancat and Dr Hasyim Gautama for supporting me during my studies at Oxford University.

I thank my colleagues both in Oxford and back home (KOMINFO), and all the members of the Trustworthy Systems Group (Ranj, Ahmad, Pardeep, Robin, Ravi and others) and the Security and Privacy Reading Group, for the many stimulating discussions we have had. I also thank, Dr Pardeep Kumar, Dr Wamala and Kim Anderson for valuable reviews and feedback. Special thanks to Maureen, David and Jackie for their kind support during my study at Oxford.

I am grateful to those who have supported my DPhil financially: the Indonesian Government through the Indonesia Endowment Fund for Education (LPDP). Travel funding from CDT in Cyber Security, Linacre College and the Department of Computer Science. I also appreciate the kind support from the Directorate of Information Security - KOMINFO.

I have had the privilege of meeting many amazing people during my time in Oxford, and so I thank all my friends from the CDT in Cyber Security, LPDP-Oxford, PPI Oxford, OXONIS, Linacre College, OII and the Department of Computer Science for all the memorable occasions we have shared.

Special thanks to my beloved wife and sons for their sacrifice throughout this adventure and for accompanying me for the duration of the study, and making the UK our second home. Finally, thank you so much to my surviving mother for her love, pray, support and wise advice. To my late father who passed away during my writing of this thesis and left an empty space in my life that time cannot fill, thank you for love and care you gave me, for your prayer, advice, inspiration, and support which are my keys to success.

He (Allah) has taught man that which he knew not (Surah Al-Alaq Verse 5).

This thesis is dedicated to my beloved mother, wife and children, and especially for my late father (Drs. H. Yusrip Achmar, S.E., M.M.) who unfortunately didn't stay in this world long enough to see his son become a Doctor of Philosophy (DPhil).

Definitions

External Information System Service (NIST SP 800-53 Revision 4) [1]	An information system service that is implemented outside of the authorisation boundary of the organisational information system (i.e. a service that is used by, but not a part of, the organisational information system) and for which the organisation typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider (NIST SP 800-53 Revision 4) [1]	A provider of external information system services to an organisation through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e. through contracts, inter-agency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
Confidentiality(NIST SP 800-53 Revision 4) [1]	Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Assurance(NIST SP 800-53 Revision 4) [1]	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Trustworthiness(NIST SP 800-53 Revision 4) [1]	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

Abbreviations

SLA	Service Level Agreement
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
DoD	Department of Defense (US)
FedRAMP	The Federal Risk and Authorization Management Program
HIPAA	Health Insurance Portability and Accountability Act (US)
FIPS	Federal Information Processing Standards
SOC	System and Organisation Controls
CSA	Cloud Security Alliance
AWS	Amazon Web Services
DoD SRG	Department of Defense Cloud Computing Security Requirements Guide
FISMA	Federal Information Security Management Act
BSI	the German Federal Office for Information Security
C5	Cloud Computing Compliance Controls Catalogue

Contents

List of Figures

List of Tables

1
Introduction

> *Unlike the insurance industry, which can predict its level of exposure to a particular class of threat, the assurance industry can not quantify the potential exposure of a given system to a given class of threats. Rather, security risks tend to behave and propagate more like infectious epidemics, as opposed to a controllable, predictable manner.*

Ronda R. Henning, *Security Service Level Agreements*, 1999

Contents

1.1 Motivation

During the years preceding and this study, government agencies have been targets from a wide range of cyber attacks, by perpetrators with capabilities ranging from least sophisticated to most sophisticated. According to data from BAE Systems, 67% of the cyber attacks have targeted government agencies, and followed by embassies (15%), technology company (7%), international organisation (6%) and academic institute (5%).[1] The Control Risks support this statistical data on Risk Map Report 2016 [4]. The report points out that the government sector is the top sector targeted by cyber attacks (36% of total attacks), followed by the financial sector (26%), telecommunications (16%), the retail industry (14%) and the oil and gas sector (8%). Such figures are somehow not surprising because government agencies generate, collect and store far more sensitive data than private sector organisations [5]. Based on such data, it seems that governments around the world are constantly under targeted attacks [4, 5].

Further, these cyber threats are generated by internal and external factors to government agencies. For example, an attacker can access government data stored into the web server and steal sensitive data [6]. Moreover, it is becoming apparent that the greatest threats to organisational security stem from insider threats [7] - that is - from, those who routinely work with government agencies (including employees, contractors, business partners and service providers). It has become clear that government agencies are regularly targeted by perpetrators ranging from unskilled individuals (e.g. script kiddies) to sophisticated and well-funded adversaries (e.g. foreign intelligence services) [5]. This point is supported by evidence concerning the secret documents made public by Edward Snowden about alleged pervasive surveillance attacks posed by foreign intelligence services, such as the US National Security Agency (NSA) and its counterparts such as Australian Signals Directorate (ASD) particularly to the Indonesian Government [8–12].

This thesis is motivated to gain a deeper understanding of the problem of protecting sensitive government data following alleged comprehensive unauthorised access by ASD to Indonesia's national communications systems. Such unauthorised access including moni-

[1] Data was gathered from the slides presented to the Indonesian government in 2016

toring of mobile phone calls of the Indonesian president and collecting data on Indonesian officials in various government ministries in 2013 [9, 10]. Australian intelligence agency and NSA also obtained 1.8 million encrypted master keys used to protect private communications, from Indonesia's major service provider [11, 12]. Therefore, the Government has made reasonable efforts to mitigate such threats in the future, by requiring all operators and services providers to ensure the security of all information systems including information system services from unauthorised access [8].

As a consequence, the Government relies on the experience of operators and service providers to mitigate unauthorised access to Indonesia's national computing, communications and storage systems. However, the service providers claim that the security capabilities they provide are in conformity with the security standard ISO/IEC 27000 series. Some security controls of ISO/IEC 27002 that relate to such claims include: A.9.2.3 Management of Privileged Access Rights; A.12.2.1 Controls against Malware; A.13.1.1 Network Controls; A.15.1.2 Address Security within Supplier Agreements; and A.15.2.1 Monitoring and Review of Supplier Services. In other words, both government agencies and services providers have relied on this certification scheme to assure the security of data and information systems against unauthorised access, disclosure, modification, disruption or destruction [13, 14].

Many certification schemes have become essential for government procurement and tender processes to help identify levels of security for information systems [15] because measuring levels of security products, systems, and services is a hard problem [16, 17]. For example, Common Criteria (CC) is often used as the basis for a government-driven certification scheme and security evaluation for information technology products and systems [18]. Such a certification scheme is designed for public procurement to certify levels of security for products that range from hardware to software and firmware [15, 19].

However, the CC certification is an expensive process and known to be slow-moving as evaluation takes up to 12 months [19, 20]. Additionally, the CC certification only focuses on the technical elements of the products and systems, while other security elements, such as administrative and legal aspects, are overlooked [19]. Moreover, the certification of commercial products is questionable because the contexts of application are different from those used to evaluate the products [19]. These flaws can be a direct consequence of a lack of

interest from service providers to seriously consider the CC certification scheme for services. Although several studies have examined the application of CC to service scenarios [20, 21], very few services make use of the CC certification scheme [21, 22]. Consequently, it can be argued that such a certification is inappropriate in the context of service provision.

Another certification for public procurement is based on the industry standard ISO/IEC 27001 [15, 19]. Such certification is a requirement for public procurement-related services and information technology systems for Indonesian government agencies [13]. However, it is apparent that the certification scheme is intended for certifying information security management system (ISMS) for a specific scope, but not suited to addressing emerging threats and vulnerabilities. Rather, it is more likely to ensure compliance with a particular security standard, than achieve a significant level of security for products, systems and services [15, 19, 23]. Overall, this explains that certification schemes to both products and services face a problem with a dynamic threat environment. It can be concluded that the certification schemes are not well-suited to the service scenario because certifications do not fit into a dynamic threat environment [24].

Based on the above problems, this research aims to investigate the concept of assurance and trustworthiness when using external information system services, such as cloud-based services. To this end, this thesis introduces the concept of a Trustworthy Data Security Level Agreement (TDSLA) Capability Framework as a practical assurance approach for enhancing trust and security in dynamic service provisioning environments. The inspiration for building such a framework is the adaptability of the CC certification process.

In this thesis, such a framework is developed using three qualitative studies that incorporate views from government and service provider experts. Central to the proposed framework is discrete security assurance levels that can be incorporated into a service level agreement. Formulating discrete security assurance levels are correlated with the main categories of classifying government data, identifying data confidentiality risks, defining SLA data confidentiality requirements, and provisioning data confidentiality capabilities. Each level of security assurance is distinct from another and offers an increase in the protection against a broader class of threats than the previous level. Thus, the framework developed can set the process to deal with dynamic threats in increasingly global computing environments.

1.2 Research Problem

Certification schemes have been used as the basis for assuring the security of government data and information systems against unauthorised access, disclosure, modification, disruption or destruction. Many certification schemes, such as CC, ISO/IEC 27001, PCI DSS (Payment Card Industry Data Security Standard) and UK Cyber Essentials have become essential for government procurement and tender processes to provide security assurance to government agencies [25]. However, several previous studies claim that such certification schemes aim to demonstrate compliance with a security standard, rather than achieve a specified level of security [23]. Even so, certification schemes are an expensive process and cause substantial costs to service providers [15]. Such certification procedures are mostly manual and require considerable effort and investments [26].

Many global service providers, such as AWS, Microsoft Azure, Google Cloud have used various certification schemes to assure the security of their services, and demonstrate compliance with ISO, PCI, DoD or FedRAMP [27]. Although certification schemes are widely used for procuring external information system services (e.g. cloud services), the use of certification schemes to assuring the levels of security for services have identified several problems. Besides being slow-moving processes, certification schemes are not well-suited to the service scenario because they are not designed for a dynamic environment. Further, protection profiles created based on assumptions about the target environment rather than verifiable attributes [24].

In particular, the problem is that levels of security assurance required for security controls listed in NIST SP 800-53 or ISO/IEC 27002 do not incorporate well into SLA contexts. There has been some research into expressing security parameters in SLA contexts as a means of addressing such problem [28–30]. The approach taken by previous research is to incorporate security controls from NIST 800-53 and ISO/IEC 27002 into SLAs, which thus constitute a security-related SLA. While such studies provide valuable insights into the problem of formulating and incorporating the Government's data confidentiality requirements, there remains much ground to cover in regards to the development of the concept of assurance and trustworthiness when using external information system services.

Furthermore, although the concept of security-related SLAs has been studied since 1999 [31–38], a gap still exists in the investigation of how to incorporate the Government's data confidentiality requirements into SLAs. A significant element in closing this gap is greater understanding of providing SLAs with discrete levels of security assurance based the data classification and threat model. This gap helps to inform the idea of proposing a TDSLA capability framework that incorporates the Government's data confidentiality requirements into the formulation of discrete levels of security assurance in SLAs.

The idea of a TDSLA capability framework as one of the assurance approaches used in the context of service provisioning is in line with one of the provisions of the Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012. The Government Regulation requires service providers to have agreements on minimum service level and information security when provisioning such external services to customers. However, the concept of assurance-based SLA for data security provisions is relatively new to the Government and service providers. In particular, security service metrics and provisions related to data confidentiality are not well-established.

Given the need to develop a TDSLA capability framework for Indonesia, this thesis formulates the main research question as follows:

How can the Indonesian Government's data confidentiality requirements be incorporated into a service level agreement?

This thesis addresses the question by conducting three qualitative studies that incorporate views from government and service provider experts. As a result of empirical qualitative studies, principles for building a TDSLA capability framework are developed and validated. For this purpose, the main research question (RQ) can be broken down into the following sub-questions (SQs):

- **SQ1**: What are the Government security needs for protecting sensitive government data against unauthorised access?
- **SQ2**: What are the understandings of government SLA data confidentiality requirements when using external information system services?

- **SQ3**: What are the current and potential future provisions for data confidentiality in SLAs provided by external service providers to Indonesian government agencies?

This thesis examines each of these sub-questions in a series of empirical studies. An overview of how these sub-questions are addressed in this thesis is provided in Section 1.7.

1.3 Research Scope

The following scope and limitations are applied to this thesis.

- This research focuses on the problem of protecting sensitive government data after the secret documents made public by Edward Snowden. The provenance and accuracy of those documents cannot, of course, be independently verified; however, this has not been substantially challenged. Therefore, for this thesis, the researcher assumes that the claims arising from this evidence are accurate.

- This thesis focuses on the Government's data confidentiality requirements. Other security requirements, such as data integrity and data availability, are not included in this thesis. Potential adversaries include active or passive adversaries, adversaries from an external or internal entity to the system and adversaries from a single entity or a well-funded nation-state. Such adversaries mainly aim at attempting unauthorised access to any sensitive data that is processed, stored or transmitted.

- A significant impetus for this research emerged from Article 12 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012 (Government Regulation No. 82/2012), which requires service providers to have agreements on minimum service level and information security when provisioning such external services to government agencies as customers.

- The case study of this thesis is limited to the context of the Indonesian Government; therefore, it is not applicable in other countries. Further, although SLAs can be established with various interacting entities (i.e. customers, end-users, service providers, suppliers, integrators, standards bodies and accreditation bodies), this thesis discusses

the idea of proposing a TDSLA capability framework as a means of incorporating data confidentiality requirements into SLAs between government agencies and service providers.

- This thesis does not seek to develop the basis for futuristic SLAs. Instead, this research concentrates on the development of principles emerging from the Delphi study data, which are used as foundations for the proposed framework. The scope of this study, thus, is mostly the theory development for building a TDSLA capability framework.

- This thesis does not seek to express data confidentiality requirements in legal language. Instead, it establishes discrete levels of security assurance for incorporating the Government's data confidentiality requirements into SLA contexts. Thus, the level of security assurance required and agreed can be written in legal language.

- As with any research method, there are advantages and disadvantages with using the methodology used in this thesis. These aspects are discussed in Chapter 3.

Significant scoping work is limited to external information system services. As this study was specifically interested in the context of service provision, a distinction was made between 'products' and 'services' regarding the concept of assurance and trustworthiness. Admittedly, certification schemes, such as CC and ISO/IEC 27001, are often used as the basis for assuring appropriate levels of security for services. However, such certifications are unsuitable in the context of service provision. Thus, this thesis is concerned with another assurance system using SLA-based discrete security assurance levels.

1.4 Research Approach

Real-world qualitative empirical studies investigating the Government's data confidentiality requirements are challenging. Qualitative researchers face many options for methods to generate and analyse data ranging from grounded theory, interviews, focus groups, case studies, participant observation, ethnography, content analysis, among many others [39, 40]. Such research endeavour is labour and time-consuming. Gaining access to participants

proved to be a particularly challenging aspect of this research. Few government participants, including service providers, are willing to share their experiences when it comes to the Government's security posture.

To this end, this thesis employs various research methods, namely: an adaptive Wideband Delphi study, grounded theory or combination of the Delphi method and grounded theory, called the grounded adaptive Delphi method (GADM). An adaptive Wideband Delphi method based on the traditional Delphi method and Wideband Delphi method is developed to engage with such participants as well as to minimise barriers to completing the data collection activities. This technique is one of the more practical ways of investigating the Government's confidentiality requirements by using specific Delphi features, such as controlled feedback and group responses with face-to-face meetings [14]. Thus, this thesis employs such research method to address the first sub-question (SQ1).

If the goal is to fill the gap by understanding the Government's perspective about SLA data confidentiality requirements as stated in the second sub-question (SQ2), the research approach used is a grounded adaptive Delphi method (GADM, a relatively new methodological extension of the Delphi method. It integrates aspects of grounded theory, particularly concerning the data analysis and the Delphi method as a means of iterative data collection activities. Several previous studies argue that incorporating elements of grounded theory assists in and enhances the theory capabilities of the Delphi method [41, 42]. This thesis also uses GADM to address the third sub-question (SQ3).

If the purpose is to construct principles and framework that reflect reality methods such as grounded theory can assist the discovery of theory from the data [43]. Thus, this thesis attempts to propose principles as foundations for a TDSLA capability framework between government agencies and service providers by conducting a qualitative analysis using a grounded theory approach of the two previous empirical studies (SQ2 and SQ3).

Overall, Chapter 3 provides a detailed description of this method. The chapter also provides a complete discussion about the components of the Delphi method and grounded theory and how they are combined to form the grounded adaptive Delphi method (GADM).

1.5 Ethical Considerations

Some parts of this work have received Ethical Approval from the Social Sciences and Humanities Inter-divisional Research Ethics Committee (IDREC), the University of Oxford with reference No: SSD/CUREC1A/14-065. The rest of this work conducted qualitative studies under the same ethical approval because the studies were carried out consecutively using the same research method. Furthermore, the researcher obtained informed written or verbal consent from all participants, both to participate in the study as well as to have the focus group or interviews audio recorded. Participants were told the objective of the study and asked for their involvement in the study. Participants were voluntary and anonymous, and they had the right to drop out in any round. The researcher transmitted and stored these audio files only in encrypted form. The researcher did not record or store any explicitly identifying metadata (e.g. the name of the participants or organisation), nor does the researcher report those here. Though participants were asked to reflect on the recent government's security posture, the researcher explicitly asked them not to reveal any sensitive government information. The researcher felt that the resulting Delphi data collection did not contain sensitive details.

1.6 Contributions

The thesis claims three contributions (methodological, empirical and conceptual) towards the stated sub-research questions.

- **Methodological Contribution**: The first contribution is developing and conducting an adaptive Wideband Delphi method to engage with senior Indonesian officials as well as to minimise barriers to completing data collection activities. An additional methodological contribution made in this thesis has been the application of grounded theory to the transcripts of the Delphi study data as a means of providing a higher theoretical understanding of the specific categories which constitute main components of the principles. Combining these two approaches allow the researcher to gain additional validity from the results as both methodologies complement each other. An

adaptive Delphi method is useful in obtaining a genuine understanding of the issues and the validity of the research through an iterative process and respondent validation. Grounded theory provides a robust qualitative analysis to examine the Delphi study data in more coherent concepts and categories that constitute building blocks of the principles and framework emerging from the data.

- **Empirical Contribution**: The second contribution is developing a foundation for future research by providing various understandings of government security needs, government SLA data confidentiality requirements and service provision for data confidentiality in SLAs, using Indonesia as a case study.

- **Conceptual Contribution**: The third contribution of this thesis is developing foundations for a TDSLA capability framework and validating the principles and framework which have emerged through reflection against related works, testimonial validity and application of transferability. Such principles and framework developed based on interpretation of the Delphi study data. By employing the grounded theory approach, this thesis presents five principles as buildings block of the proposed framework. Another contribution is a critical review of the State-of-the-Art concerning the inclusion of data confidentiality considerations in SLA contexts.

1.7 Thesis Structure

Figure 1.1 provides a graphical representation of the structure of this thesis and describes how its structure maps to the research question and the sub-research questions and how these questions work to develop the thesis contributions.

Chapter 1 provides a rationale for the research undertaking by presenting a discussion of the research problem followed by a statement of the research questions. Research approach, contributions follow the research scope to further contextualise this study.

Chapter 2 provides a background of the concepts of trust and trustworthiness in the context of a service provisioning environment. This chapter then describes an overview of data confidentiality issues, including understanding government security needs, government

SLA data confidentiality requirements, service provision for data confidentiality in SLAs and the concepts of discrete levels of assurance as elements of a TDSLA capability framework. Chapter 2 also provides a discussion of existing assurance approaches. This chapter discusses the state-of-the-art and presents a gap analysis of previous studies highlighting the research gap addressed by this thesis. The chapter concludes by discussing the choice of research methods to address the gap.

Chapter 3 outlines the methodology used in this thesis and justifies the choice made to investigate the problem of protecting sensitive data across government agencies when using external information system services supplied by external service providers. This thesis employs various research methods, such as: an adaptive Delphi study; grounded theory; and a GADM approach. This chapter also provides the specific applications of the GADM.

Chapter 4 presents a study to investigate the Indonesian Government's security needs to mitigate unauthorised access to sensitive government data in response to the problem of preserving the confidentiality of government data after the secret documents made public by Edward Snowden. The chapter reports the importance of having information security agreements when using such external services.

Chapter 5 reports the understanding of government SLA confidentiality requirements using 35 participants (government employees and government consultants) using GADM.

Chapter 6 examines the current and potential service provisions for data confidentiality in SLAs. As such, this chapter conducts a longitudinal study of government auctions to select major service providers that provide services to Indonesian government agencies. Five selected service providers with 15 participants are involved in this study.

Chapter 7 presents a qualitative study based on the grounded theory to examine the Delphi study data from the two previous qualitative studies (Chapter 5 and Chapter 6). This chapter identifies concepts and categories as central components to develop principles, thus providing a framework for building a TDSLA capability. The principles and framework which have emerged from the data are evaluated and validated.

Chapter 8 presents a summary of findings and the contributions to knowledge made by this thesis. This chapter provides discussion and limitations of the study results. The chapter also provides reflections on the research process and identifies areas for further research.

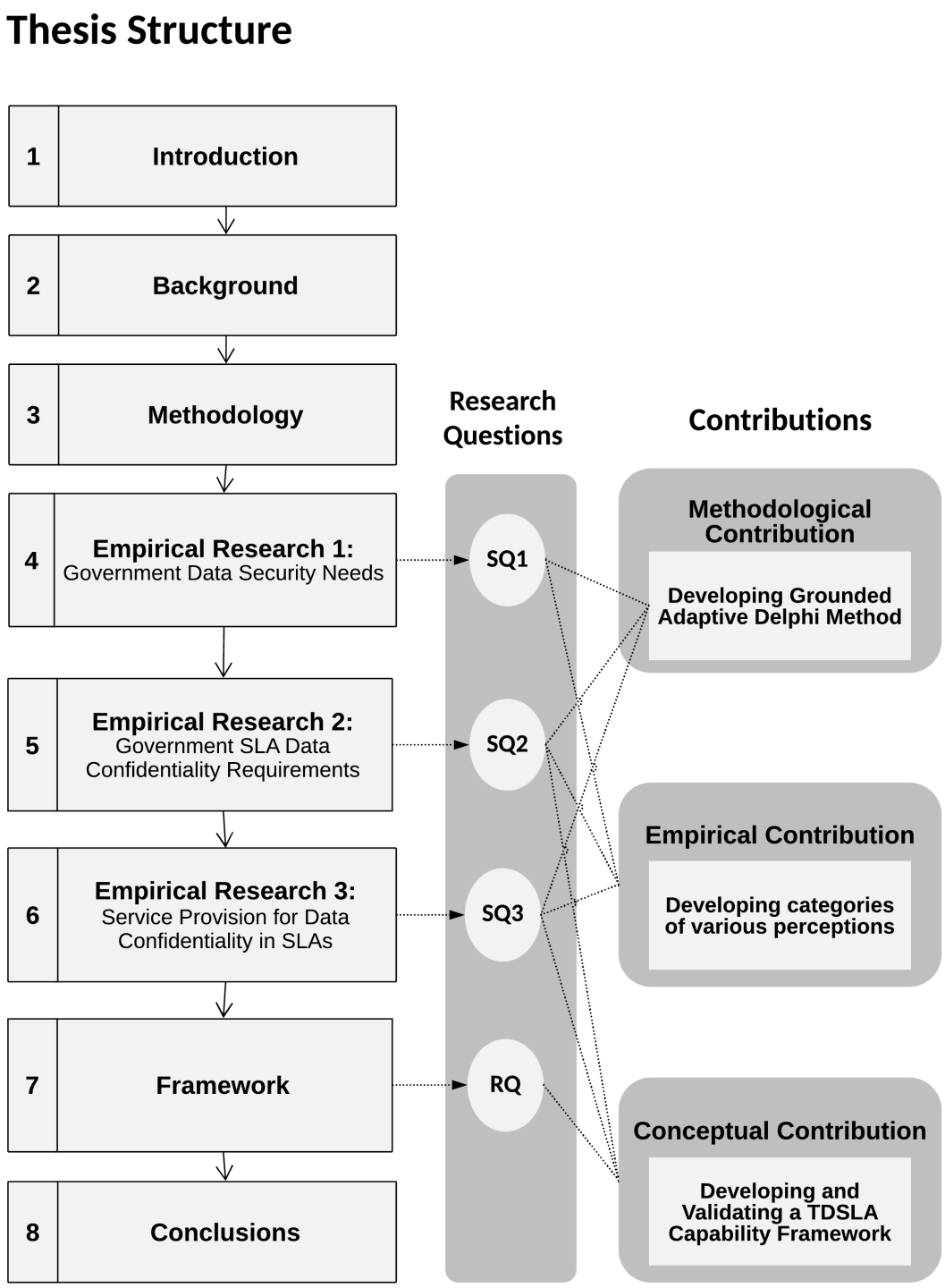


Figure 1.1: Thesis Structure

2
Background

> *Trustworthiness with respect to information systems, expresses the degree to which the systems can be expected to preserve with some degree of confidence, the confidentiality, integrity, and availability of the information that is being processed, stored, or transmitted by the systems across a range of threats.*
>
> NIST Special Publication 800-53, *Revision 4*, 2013

Chapter 2 draws on refereed articles described in the following publications:

- Y. Nugraha and A. Martin. Understanding Trustworthy Service Level Agreements. In Proceedings of IFIP WG 11.4 International Workshop on Open Research Problems in Network Security (iNetSec), Springer, 2017.
- Y. Nugraha. Security Assurance Requirements Engineering (STARE) for Trustworthy Service Level Agreements. In Proceedings of 23rd International Conference on Requirements Engineering (RE'15), pp. 398-399, IEEE, 2015

Contents

2.1 Introduction

This chapter provides background information about the major themes that are relevant to this thesis. Section 2.2 provides background to notions of trust and trustworthiness in the context of a service provisioning environment. The section explores the concept of assurance-based service level agreements (SLAs) as trust-enhancing instruments between government agencies and service providers. Further, Section 2.3 provides an overview of data confidentiality issues, including an understanding of government security needs, government SLA confidentiality requirements, service provision for confidentiality in SLAs and discrete levels of security assurance. These understandings create the basis of trustworthiness model as foundations for building a TDSLA capability framework. Section 2.4 then provides a discussion of existing assurance approaches for establishing trust and trustworthiness in a service provisioning environment including SLAs. The next section (Section 2.5) presents the context of the need for security-related SLAs when procuring external information system services, using Indonesia as a case study. The two following sections discuss respectively the state-of-the-art security-related SLAs and the research gap that this thesis addresses. The chapter concludes by discussing the choice of research method to address the research gap.

2.2 Trust and Trustworthiness

Despite the apparent similarity, the terms 'trust' and 'trustworthiness' have distinct meanings depending on the context in which they are used. According to the NIST SP800-53 guideline [1], *trust* can be defined as '*the belief that an entity will behave in a predictable manner while performing specific functions, in specific environments, and under specified conditions or circumstances*'. Such an entity can be a person, process, information system, system component, a system of a system or any combination thereof [1].

From a security perspective, '*trust is the belief that a security-relevant entity will behave in a predictable manner when satisfying a defined set of security requirements under specified conditions or circumstances and while subjected to disruptions, human errors,*

component faults and failures, and purposeful attacks that may occur in the environment of operation' [1]. In other words, *trust* is the belief that a security-related entity will behave as expected, according to the required security requirements, which defined based on a risk tolerance level. Thus, this definition implies that trust can be determined by a specific security capability, which is a combination of security controls to be applied against threats. Such controls can stem from technical, physical and procedural means.

Whereas the term trustworthiness expresses '*the degree to which the systems can be expected to preserve with some degree of confidence, the confidentiality, integrity, and availability of the information that is being processed, stored or transmitted by the systems across a range of threats*' [1]. A trustworthy system also can be defined as '*a system that not only is trusted but also warrants that trust because the system's behaviour can be validated in some convincing way, such as formal analysis or code review*' [44]. In other words, trustworthiness can serve as an assurance that a system will perform as expected [45].

This thesis focuses on the concept of system assurance and trustworthiness in a service provisioning environment. In essence, developing foundations for a TDSLA capability framework is in line with the understandings of government security needs, government SLA security requirements, service provision for security in SLAs, and the formulation of discrete security assurance levels in the context of SLA. Figure 2.1 illustrates the main categories affecting a TDSLA capability framework. The trustworthy model promotes traceability from data security needs to SLA data security requirements to service provision for security with discrete security assurance levels.

Trustworthiness is a holistic property, encompassing data security (data confidentiality, data integrity and data availability). Given this study's specific interest in the protection of sensitive government data, this thesis focuses on data confidentiality. The work on the Indonesian Government's data confidentiality requirements guides to develop principles and framework from the collected data.

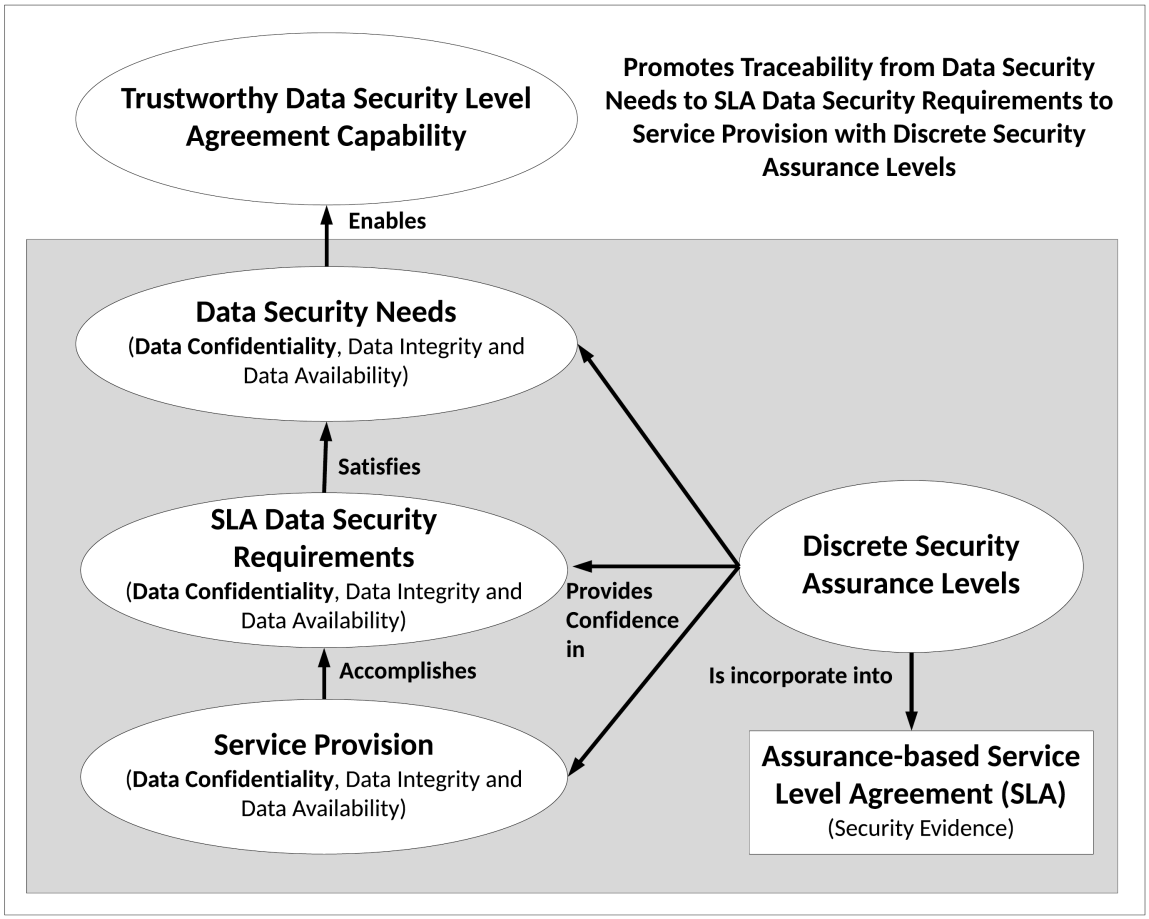


Figure 2.1: Trustworthiness Model—Adapted from NIST 800-53 [1]

2.3 Data Confidentiality

Confidentiality is one property of the CIA (Confidentiality, Integrity, and Availability) Triad security model [46]. According to NIST SP 800-171, confidentiality is the notion of 'preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information' [47]. In other words, confidentiality covers two related notions of data confidentiality and privacy [48]. This thesis focuses on the inclusion of the Government's data confidentiality requirements into SLAs. The definition of data confidentiality service can serve as an assurance that any sensitive government data is not accessed or made available to unauthorised individuals, entities or processes.

In the broader context of government supply chains, ensuring data confidentiality is often placed on what sensitive data is not allowed to disclose to third parties through a confidentiality agreement, also known as a non-disclosure agreement (NDA). The NDA agreement is a legal contract between two or more parties that outlines the parties involved agree not to disclose sensitive information covered by the agreement [49]. However, the NDA agreement is expressed in natural language and does not express specified levels of security required to protect sensitive government data. For example, all parties are expected not to disclose any sensitive data without achieving an adequate level of security required to address risks to unauthorised access. Thus, the NDA contract is not well-suited to service provisioning environments, especially when using external information system services.

In the service scenario, an SLA has been used to established business relationships with service providers in various service and outsourcing scenarios. An SLA can serve as a binding agreement between a service provider and a customer to define and manage levels of service provided in qualitative and quantitative terms based on understandings of customer requirements and service provider capabilities [33, 50]. However, existing understandings of SLAs are focused on the performance and system availability aspects without considering data security, such as data confidentiality, data integrity, data availability in SLA contexts [33, 34]. Therefore, it is worthwhile to investigate how to incorporate the Government's data confidentiality requirements into SLAs.

The following subsections provide background on essential concepts of government security needs, government SLA data confidentiality requirements, service provision for data confidentiality in SLAs and levels of security assurance that can serve as discrete qualitative metrics in the formulation of assurance-based SLA.

2.3.1 Government Security Needs

Security needs differ from security requirements. According to Thompson [51], a requirement is '*a statement which translates or expresses a need and its associated constraints and conditions*'. Borrowing the definition from Turpe [52], '*security requirements express security needs in a form suitable to inform security design and make its results variable*'.

In practice, government security needs can be found in national laws, policies, regulations, standards, procedures and guidelines [1]. Whereas security requirements are derived from government security needs to ensure confidentiality, integrity and availability of the information being processed, stored, or transmitted by organisational information systems [1].

There is no formal definition of the government's security needs. This subsection discusses the following studies to understand the notion of government security needs against disclosing sensitive government data. Several authors have published studies on government responses to preserving the confidentiality of sensitive data against unauthorised access, in particular, pervasive surveillance attacks posed by foreign intelligence service [53].

According to Feigenbaum and Koenig [54], one primary enabler of pervasive surveillance is the commerciality of ad-supported cloud services, which are centralised services. However, such services have problematic consequences, such as the loss of confidentiality and the ease of pervasive surveillance. Thus, building decentralised global-scale cloud services using open-source platforms is a potential requirement for the future decentralised Internet.

Similarly, Bauman et al. [55] outline some government security needs from the German and Brazilian governments against pervasive surveillance attacks. These security needs include the creation of local data clouds, national Internet routing, development of surveillance capabilities, investment in security professionals and intelligence experts. Both governments have attempted to develop domestic content and infrastructure, such as local social media platforms, national email services as well as international Internet backbones beyond the scope of the US-based Internet infrastructure. It appears that the secret documents made public by Edward Snowden have engendered distrust in many countries outside the UKUSA alliance (the U.S., the U.K., Canada, Australia and New Zealand).

Likewise, Rubinsstein and Van Hoboken [56] point out that some governments impose legal requirements on cloud-based services aimed at preventing unauthorised access and requiring local storage of sensitive data inside the country. Such security efforts are launched to resist the NSA's PRISM (Planning Tool for Resource Integration, Synchronization, and Management) program under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008. For example, the NSA has front-door access and backdoor access to the data handled by the U.S cloud service providers through MUSCULAR to

intercept unencrypted data traffic between cloud service providers' data centres.

From a perspective of the U.S. government, Toxen [57] proposes some security measures and requirements which are useful for the NSA agency to prevent an insider like Edward Snowden from stealing sensitive government data. The author argues that many of these security measures have been in use for some time. The following provides detail requirements for the NSA agency [57]:

- The agency should treat any systems as different islands of security, which have different root passwords, different user passwords, different SSH (Secure Shell) passphrases, and all traffic between systems should be encrypted.

- The agency should control physical access to devices against unauthorised access. For example, two people are required to access peripherals or hardware devices, and the installation of video cameras is necessary for high-security operations.

- The agency should prohibit the use of unauthorised storage devices, such as USB (Universal Serial Bus) memory sticks, blank DVDs (Digital Video Discs), cameras, recorders and mobile phones.

- The agency should make use of multifactor authentication, such as a fingerprint and password to prevent an unauthorised user from impersonating others.

- The agency should make use of public key encryption to prevent unauthorised access. For example, the agency should have a public-private key pair created for each system administrator requiring transfer data and a separate account for each computer for each system administrator to transfer such data.

It is clear that most of the security practices mentioned above are examples of possible security needs governments can take to guard against unauthorised access [54–57]. However, there has been little empirical research into studying the Government's security needs to mitigate such threats. To this end, Chapter 4 investigates the Indonesian Government's need to mitigate unauthorised access to sensitive government data after the publication of secret documents by a former NSA contractor Edward Snowden [8–12].

2.3.2 Government SLA Data Confidentiality Requirements

Many governments around the world increasingly rely on external information system services supplied by service providers to process, store or transmit sensitive data on behalf of government agencies [58, 59]. Several governments have addressed security issues within supplier agreements. For example, the UK and US governments have taken steps to reduce the level of cybersecurity risk, especially for government procurement of external information system services [59, 60]. However, an understanding of government SLA data confidentiality requirements is a little known. Thus, this subsection provides the context for this study by examining government procurement requirements from a security perspective.

The analysis begins with the 2014 introduction by the UK government of a set of cybersecurity requirements, called Cyber Essentials (CE). CE developed in collaboration between the Government, industry and standard bodies. Under ten steps of guidance five requirements are defined [59]. The CE scheme is necessary for suppliers or service providers who want to conduct business with the UK government. The following five technical requirements are identified to mitigate common successful cyber-attacks, such as malware, phishing, and unpatched software in such an organisation, as shown in Table 2.1.

Table 2.1: Requirements for Basic Technical Protection from Cyber Attacks

No	Requirement	Description
1	Boundary Firewalls and Internet Gateway	Information, applications and computers within the organisation's internal networks **should** be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.
2	Secure Configurations	Computers and network devices **should** be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.
3	User Access Control	User accounts, particularly those with special access privileges (e.g. administrative accounts) **should** be assigned only to authorised individuals, managed effectively, and provide the minimum level of access to applications, computers and networks.
4	Malware Protection	Computers that are exposed to the Internet **should** be protected against malware infection through the use of malware protection software.
5	Patch Management	Software is running on computers and network devices **should** be kept up-to-date and have the latest security patches installed.

It shows that the five requirements listed in CE serve as the basis upon of which specific security controls define. However, Heitzenrater and Simpson [61] found that the specified technical controls do not map directly to specific threats. For example, some technical controls, such as firewall and patching can mitigate attacks by unauthorised outsiders.

In the context of cloud computing, another UK initiative also outlines 14 cloud security principles, as shown in Table 2.2 [62]. Such principles are cloud security requirements for government agencies that want to procure cloud-based services from service providers. Each principle represents a fundamental security aspect that is essential when selecting cloud services. For example, Amazon Web Services (AWS) listed on the G-Cloud Framework can provide cloud services to government agencies [58]. For this purpose, AWS provides insights into an implementation approach based the 14 cloud security principles to make an informed decision when selecting the cloud services for handling government data classified as official information [58].

Table 2.2: Cloud Security Principles

No	Requirement	Description
1	Data in Transit Protection	User data transiting networks ***should*** be adequately protected against tampering and eavesdropping.
2	Asset Protection and Resilience	User data, and the assets storing or processing it, ***should*** be protected against physical tampering, loss, damage or seizure.
3	Separation between Customers	A malicious or compromised user of the service ***should*** not be able to affect the service or data of another.
4	Governance Framework	The service provider ***should*** have a security governance framework which coordinates and directs its management of the service and information within it.
5	Operational Security	Good operational security ***should*** not require complex, bureaucratic, time consuming or expensive processes.
6	Personnel Security	The service provider ***should*** subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities.
7	Secure Development	Services ***should*** be designed and developed to identify and mitigate threats to their security.
8	Supply Chain Security	The service provider ***should*** ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.
9	Secure Customer Management	The service provider ***should*** make the tools available for you to securely manage your use of their service.
10	Identity and Authentication	All access to service interfaces ***should*** be constrained to authenticated and authorised individuals.
11	External Interface Protection	All external or less trusted interfaces of the service ***should*** be identified and appropriately defended.
12	Secure Service Administration	The design, implementation and management of administration systems ***should*** follow enterprise good practice, whilst recognising their high value to attackers.
13	Audit Information Provision to Customer	A customer ***should*** be provided with the audit records needed to monitor access to your service and the data held within it.
14	Secure Use of the Service	A customer ***should*** have certain responsibilities when using the service in order for your data to be adequately protected.

In the context of the US government procurement policy, any potential and existing suppliers, service providers or contractors working with the federal agencies are required to meet 14 security requirements described in the NIST SP 800-171 standard [47, 60], as shown in Table 2.3. The 14 security requirements aimed at protecting the confidentiality of any information that must be adequately protected under all applicable laws, regulations or government policies [47].

Table 2.3: Confidentiality Requirements for Government Contractors

No	Requirement	Description
1	Access Control	Limit information system access to authorised users, processes acting on behalf of authorised users, or devices
2	Awareness and Training	Ensure that organisational personnel are made aware of the security risks associated with their activities
3	Audit and Accountability	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
4	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organisational information systems.
5	Identification and Authentication	Identify information system users, processes acting on behalf of users, or devices
6	Incident Response	Track, document, and report incidents to appropriate organisational officials and/or authorities.
7	Maintenance	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
8	Media Protection	Protect information system media containing CUI, both paper and digital.
9	Personnel Security	Screen individuals prior to authorising access to information systems containing CUI.
10	Physical Protection	Limit physical access to organisational information systems, equipment, and the respective operating environments to authorised individuals
11	Risk Assessment	Periodically assess the risk to operations, assets, and individuals.
12	Security Assessment	Periodically assess the security controls in organisational information systems to determine if the controls are effective in their application.
13	System and Communications Protection	Monitor, control, and protect organisational communications at the external boundaries and key internal boundaries of the information systems.
14	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.

Furthermore, the NIST guideline provides government agencies with minimum security requirements for protecting the confidentiality of controlled unclassified information (CUI) when using external information system services [1, 47]. For example, the guideline is necessary for suppliers or service providers that want to offer external services to government agencies, when the offered services are relying on private cloud-based services to process,

store or transmit sensitive government data [63]. However, another guideline, the Federal Risk and Authorization Management Program (FedRAMP), is required when such suppliers or service providers use external cloud-based services to handle government data [64].

When procuring services from service providers, public procurement policy in the UK and the US exhibits mixed evidence of the incorporation of security considerations. Although the UK government does not specify specific data confidentiality requirements that should be met by service providers [62], government agencies can procure and use cloud-based services for handling government data classified as official information.

However, the US government provides minimum confidentiality requirements for preserving the confidentiality of CUI which replaces categories *For Official Use Only* and *Sensitive But Unclassified*. The confidentiality requirements are required when suppliers or service providers process, store or transmit sensitive data in their information systems.

Even so, more discussion is necessary on how such data confidentiality requirements can be incorporated into SLAs between government agencies and service providers. This understanding provides an impetus for further investigation into better specifying data confidentiality requirements into government SLAs. Therefore, Chapter 5 investigates the practical application of government SLA confidentiality requirements to the case of the Indonesian Government by drawing on government employees' expertise in security areas such as information security management, cryptography, cyber defence, malware and penetration testing.

2.3.3 Service Provision for Data Confidentiality in SLAs

A data confidentiality service is a notion of preventing unauthorised access or disclosure of sensitive data (either processed, stored or transmitted) [1]. In the provision of the data confidentiality service, many variables can be identified, such as the location of sensitive data, the classification of sensitive data and the value of sensitive data [65]. This subsection examines the security controls catalogues to identify and understand data confidentiality capabilities, namely: ISO/IEC 27002:2013; NIST SP 800-53; and the Centre for Internet Security's 20 Critical Security Controls.

One of the security standards that widely used by many government agencies is the ISO/IEC 27002:2013 standard. This standard replaces ISO/IEC 27002:2005. Reflecting the fact that many organisations rely on third-party suppliers to provide information system services, it is noteworthy that the updated standard details additional controls on outsourcing [66]. The 2013 standard contains 114 detailed controls in 14 domains with 35 control objectives. The 2005 standard consisted of 133 controls in 11 domains.

Further, the ISO 27002 standard is a guideline for implementing security controls to help ensure the defined security objectives achieved. The approach applies a "check-list" of controls that auditors can use to assess compliance with the standard [18]. However, the standard has limited security controls that address emerging risks and threats from unauthorised access or disclosure, as shown in Table 2.4.

Table 2.4: Examples of Data Confidentiality Capabilities (ISO/IEC 27002:2013)

Control	Capability	Description
Classification of information	Procedure	Information **shall be** classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
Physical media transfer	Physical	Media containing information **shall be** protected against unauthorised access, misuse or corruption during transportation.
Information access restriction	Procedure	Access to information and application system functions **shall be** restricted in accordance with the access control policy
Policy on the use of cryptographic controls	Procedure	A policy on the use of cryptographic controls for protection of information **shall be** developed and implemented.
Key management	Technical	A policy on the use, protection and lifetime of cryptographic keys **shall be** developed and implemented through their whole lifecycle.
Physical entry controls	Physical	Secure areas **shall be** protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
Controls against malware	Technical	Detection, prevention and recovery controls to protect against malware **shall be** implemented, combined with appropriate use awareness.
Protection of log information	Technical	Logging facilities and log information **shall be** protected against tampering and unauthorised access.
Network controls	Technical	Networks **shall be** managed and controlled to protect information in systems and applications.

The NIST SP 800-53 is a risk-based security standard which is intended for US federal agencies and those conducting business with the US government. The NIST SP 800-53 guideline provides a catalogue of security and privacy controls for all US federal information systems and organisations except those related to the national security [1]. The NIST standard guides federal agencies on implementing appropriate security controls. The controls consist of 18 security controls which categorise into three security control baselines based on low, moderate or high impact. Such security controls help ensure government agencies and contractors meet the security requirements set by the Federal Information Security Management Act (FISMA) [67] which is essential to any component of an information system that processes, stores or transmits government data.

However, the NIST guideline does not directly address specific issues of procuring services, even though it offers a comprehensive set of requirements for procuring secure software [68]. Although NIST SP 800-53 addresses a diverse set of security and privacy controls, it does not directly prioritise critical controls that address specific issues of preserving data confidentiality. However, Table 2.5 shows that some security controls presented in the NIST SP 800-53 guidelines can be used to protect sensitive government data from unauthorised entities.

Another set of security controls is the Critical Security Controls (CSC) developed by the Centre for Internet Security [69]. The controls are a recommended set of high-priority technical security measures and controls based on a consensus list of the best defensive techniques available to detect, prevent, respond, and mitigate harm from the most common attacks to the most pervasive and advanced attacks. The group of security experts from NSA Red and Blue team, the US Department of Energy, the US law enforcement agencies and incident response organisations developed the list of critical security controls as a set of best practices guidelines for effective cyber defence. Table 2.6 shows that some critical security controls, such as data protection, controlled access based on the need to know, malware defences, and boundary defence, are concerned with the protection against unauthorised access to data.

In conclusion, service provision based on such security standards like ISO/IEC 27002 and NIST 800-53 implies that the level of security achieved is limited to a binary consideration

Table 2.5: Examples of Data Confidentiality Capabilities (NIST SP 800-53)

Control	Capability	Description
Security Categorisation	Procedure	The organisation categorises information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
Media Transport	Physical	The organisation restricts the activities associated with the transport of information system media to authorised personnel.
Access Enforcement	Procedure	The information system enforces approved authorisations for logical access to information and system resources in accordance with applicable access control policies.
Cryptographic Protection	Technical	The information system implements [Assignment: organisation-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Cryptographic Key Establishment and Management	Technical	The organisation establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organisation-defined requirements for key generation, distribution, storage, access, and destruction].
Physical Access Control	Physical	Escorts visitors and monitors visitor activity [Assignment: organisation-defined circumstances requiring visitor escorts and monitoring].
Malicious Code Protection	Technical	The organisation employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
Protection of Audit Information	Technical	The information system protects audit information and audit tools from unauthorised access, modification, and deletion.
Transmission Confidentiality and Integrity	Technical	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

of, whether a service or system is compliant or non-compliant with such a standard. More discriminating levels of security assurance are required to articulate better the nature of the gap that separates the binary assessments of 'compliance from non-compliance' or 'secure from insecure'.

Furthermore, elements of data confidentiality provide a basis by which this more discriminating definition of service provision could be achieved to span various service provision levels. However, there has been a little empirical study into the perception of data confidentiality services in SLA contexts to elaborate much further on this assertion. Therefore, Chapter 6 investigates an understanding of service provision for data confidentiality in SLAs among selected service providers that provide information system services to Indonesian government agencies.

Table 2.6: Examples of Data Confidentiality Capabilities (20 CSC)

Control	Capability	Description
Data Protection	Technical	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
Controlled Access Based on the Need to Know	Technical	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
Malware Defenses	Technical	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defence, data gathering, and corrective action.
Maintenance, Monitoring, and Analysis of Audit Logs	Technical	Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.
Boundary Defense	Technical	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

2.3.4 Discrete Security Assurance Levels

Measuring security is difficult because security is not an event or an object, but a process [70]. However, this does not imply that measuring security is impossible. Arguably, as the measurement is essential to enhancing security, there is considerable interest in achieving such measurement for data confidentiality and determining unauthorised access to services [17]. According to Lord Kelvin[1] '*If you can not measure it, you can not improve it*'.

Many researchers suggest that feasible security metrics implement quantitative scales (e.g. numbers) rather than qualitative scales (e.g. high-low-medium ratings) [71]. However, many government agencies make use of qualitative scales for measuring 'intangible' factors, such as risk assessment. Therefore, qualitative scales, such as discrete security assurance levels, can be a practical way of formulating and classifying the Government's data confidentiality requirements according to perceived threats to sensitive government data. In this thesis, discrete security assurance levels play an essential role in defining and incorporating data confidentiality considerations into SLAs.

Many security frameworks have used various forms of levels of assurance, such as Common Criteria, ISA99, FIPS 142-2 and NIST 800-63. Common Criteria (CC) is often

[1]Lord Kelvin, PLA, Vol. 1, Electrical Units of Measurement, 1883-05-03

used as the basis for government-driven certification schemes [22]. The CC certification aims to evaluate and certify products and systems in a predefined set of categories, each with different security requirements [72]. The evaluation process defines a 'target of evaluation' and a protection profile and submits the former for evaluation against the last profile [18].

Furthermore, the security assurance requirements are grouped into seven evaluation assurance levels, labelled EAL1 through EAL7. The requirements of EAL1 afford the lowest level of assurance, and those of EAL7 afford the highest level of assurance. The evaluation assurance levels are cumulative. For example, the requirements of EAL(n+3) include those of EAL(n), EAL(n+1), and EAL(n+2). The CC certification is possible at different levels, depending upon the demonstration of compliance with security requirements. However, CC has been criticised as highly bureaucratic rather than providing genuine security enhancement [19], as it carries the cost of maintaining such a certification scheme.

Similarly, the International Society of Automation (ISA99) on security for industrial automation and control systems has highlighted the relevance of security assurance levels [73]. Such a standard defines four security assurance levels (SAL1 - SLA4), each with an increasing level of security according to the type of threat actors. For example, SAL1 is intended for protecting against casual violation, and SAL4 aims at protecting against sophisticated means with extensive resources. SALs are identified based on the seven fundamental requirements [73], namely: access control; use control; data integrity; data confidentiality; restriction of data flow; timely response to an event; and resource availability. Each requirement defines four SALs against four different level of threats (casual attackers, unsophisticated attackers, sophisticated attackers and sophisticated attackers with extensive resources). However, the level of security for each requirement lacks technical requirements regarding the strength of the security level provided to mitigate different levels of threats.

FIPS 140-2 also defines technical requirements for four security levels for cryptographic modules to protect sensitive data [74]. Four levels of security are specified for each of 11 requirement areas, such as cryptographic module specification, physical security, and key management [74]. Each provides an appropriate level of security protection according to the security requirements. This work needs to elaborate on such requirements to formulate the incorporation of discrete levels of security assurance into SLAs.

Another perspective comes in the electronic authentication guideline of NIST SP 800-63-2 [75]. This guideline defines technical requirements for each of four levels of identity assurance regarding the consequences of authentication errors and misuse of credentials [75]. Level 1 identifies the lowest assurance level, and Level 4 is the highest. The NIST 800-63 standard states specific technical requirements in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions. Each level has different threat models and offers an increase in assurance over the previous level. This standard guides on how government agencies and service providers can accomplish each assurance level selection based the data classification and threat model.

Although measuring security is difficult [17], it is clear that the formulation and classification of the Government's data confidentiality requirements are essential to assess what is being claimed and achieved by service providers that provide external information system services to government agencies [18]. In so doing, government agencies can select an appropriate level of security assurance and understand service capabilities regarding security provided by service providers.

Overall, there are significant concerns about the lack of assurance and techniques to quantify security, as well as how to classify the Government's data confidentiality requirements according to the data classification and threat model in SLA contexts. To this end, the research work in this thesis adapts the idea of levels of assurance described in the above approaches as key inspirations for formulating discrete security assurance levels for the incorporation of the Government's data confidentiality requirements into an SLA.

2.4 System Assurance

The term assurance is a much broader notion than security, which is defined as the protection of information and information systems from unauthorised access, disclosure, modification, disruption or destruction [1]. Assurance properties are aspects of the systems that can be established using evidence provided by the system or a third party [76]. These aspects may include security requirements, capabilities or functionality of the systems involved [1].

In the context of service scenarios, it is possible to have an adequate level of security and inappropriate assurance, while an inappropriate assurance technique is in line with

inadequate security levels [50]. Consequently, inadequate assurance proves that security properties are not well implemented according to laws and regulations. Many assurance approaches have been used to verify the security of a product, service or system. Those approaches include testing, monitoring, certification, audit/compliance, and SLA [50].

2.4.1 Testing

The first approach is testing. In the context of software testing, according to International Software Testing Qualifications Board (ISTQB) glossary, software testing is "*a process of executing a program or application with the intent of finding the software bugs*". In a service provisioning environment, such as cloud-based services, testing approaches can be grouped into four main categories, namely functional testing, performance testing, interoperability testing and security testing [77].

However, security testing presents a unique problem [72]. Most software or application flows and vulnerabilities are not corresponding to security functionality. As such, a penetration testing is the most common approach for software security of which it is a form of security testing performed by a group of experts who attack a target system, using a defined set of attack scenarios [72, 78]. Such testing is commonly used to measure software security, especially when the testing is integrated into the development process in such a way that findings can help to identify and fix the development problems [78]. However, the main problem with penetration testing is frequent failure to devise mitigation strategies to address the identified vulnerabilities in the analysed systems [78].

2.4.2 Monitoring

Monitoring is the second approach used to measuring information system services. This approach can help to increase the level of transparency in a service provisioning environment. According to NIST SP 800-94 on Guide to Intrusion Detection and Prevention Systems [79], such monitoring can be performed, as follows:

- Network-Based, which monitors and analyses network traffic flows to identify suspicious activities.

- Wireless, which monitors and analyses wireless network traffic flows and protocols to identify suspicious activities.
- Network Behavior Analysis, which identifies unusual traffic flows, such as distributed denial of service attacks, malware, and policy violations.
- Host-Based, which monitors features of a single host and the events occurring within that host for suspicious activities.

In the context of cloud services, monitoring can be performed through different layers, namely facility, network, operating system, middleware, application and the user [80]. These layers can be controlled and monitored by either the cloud customer or the cloud provider [80, 81]. However, the cloud service provider can control not all layers of monitoring. For instance, in the SaaS (software as a service) model, the cloud service provider can access all layers except the user layer. Similarly, the PaaS (platform as a service) provider does not have access to the application layer and the user layer. Whereas, the IaaS (infrastructure as a service) provider only has access to facility, network and hardware layers.

2.4.3 Audit and Compliance

The third important aspect of assurance systems is the capability of observing the product, software or service behaviour and evaluating its compliance with requirements and regulations [50]. In other words, a compliance audit aims to increase the level of trustworthiness between service providers and customers. In the context of cloud computing, Pearson [82] claims the need for an accountable cloud, which helps increase the level of trust, and support in the identification of responsibilities in case of disputes.

Doelitzcher [83] identifies three auditing categories which are security audit, privacy audit and legal audit. Each of these categories has different requirements to be fulfilled. The security audit includes requirements for malware protection, preventing unwanted software, service misconfiguration, unwanted service combination, account and login requirements, access rights and password strength. The privacy audit includes requirements, which help prevent metadata and accidental data disclosure, such as browser caches, log files, history

files and insecurely deleted files. The legal audit includes all set of compliance requirements, such as customer specific requirements and illegal contents.

It is clear that, although the approaches to information technology audit and financial audit are well-established, a cloud audit is more difficult than non-cloud systems. This challenge has caused barriers to procuring cloud-based services [84]. Armbrust et al. [84] point out that the lack of cloud audit capability raises questions about compliance with applicable laws and regulations, such as the U.S. Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) and the U.S. Sarbanes-Oxley Act of 2002 [85]. Thus, there is a need for a robust approach to implementing cloud audit that helps ensure compliance with the laws, regulations and standards concerning security aspects [86].

Another issue with compliance is that it is usually not mandatory, but voluntary. The importance of having compliance is to assure customers even though there is no legal or regulatory obligation to do so. Interestingly, according to Duncan and Whittington, compliance with security standards, such as ISO 27000 series, NIST and Cloud Security Alliance [23] is more likely to ensure compliance with a particular security standard, rather than achieve a significant level of security. This argument is supported by Anderson [19] because the certification process is a bureaucratic process and very time-intensive.

2.4.4 Certification

The fourth approach to evaluating and certifying the security properties of products, systems, services or processes is certification schemes. A certification aims to provide enough evidence that products, systems, services or processes hold some security properties and behaves as expected [50, 87]. Many certification schemes have become increasingly crucial in outsourcing and service provisioning environments, such as cloud services [27].

Certification schemes are widely used for government procurements and tenders to help assure the security of information systems, such as the Common Criteria (CC), Cyber Essential Plus, FedRAMP, FIPS Certification, ISO 27001, ISO 27017, ISO 27018, PCI DDS, SOC 1, SOC 2, SOC 3, BSI C5 and Cloud Security Alliance (CSA) [15] [27]. For instance, the CC certification is a framework that can serve as the basis for a government-driven

certification scheme and security evaluation for information technology products, software platforms, services or systems, especially those focused on high-assurance systems [18]. However, such certification schemes are known to be slow-moving and incur substantial costs for security services to the suppliers or service providers [15].

Further, according to Anisetti et al. [24], existing certification schemes (e.g. ISO 27001) are not well-suited to service provisioning environments. Although the CSA certification is established based on ISO 27001 for the third party independent assessment for the security of a cloud service provider, such certification schemes could not guarantee better security [19] as well as address dynamic threats and vulnerabilities [15].

2.4.5 Accreditation

Accreditation, certification and registration are often used interchangeably, but there is an important distinction between the three. The problem is that such terms have used in a different context altogether. The ISO Council Committee on Conformity Assessment (CASCO) has attempted to define those three terms [88], as follows:

- **accreditation**: the procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.
- **certification**: the procedure by which a third party gives written assurance (certificate of conformity) that a product, service or process conforms to specified requirements.
- **registration**: the procedure by which a body indicates relevant characteristics of a product, process or service, or particular of a body or person, in an appropriate publicly available list.

Accreditation is a formal recognition that an organisation or a person is competent to carry out specific tasks while certification is either self-declaration by a supplier or a formal evaluation by a third-party that a product, process or service conforms to a standard. The fact that organisations can be certified to a specific standard within a broad scope of product, service or process categories. Further, organisations such as service providers can be accredited for particular tasks, usually with specified capabilities. In other words,

organisations receive accreditation for specific activities whereas certification relates to the organisation as a whole or focus on a product, process or service to specified requirements.

For example, the Federal Risk and Authorization Management Program (FedRAMP) is a US example of a government implemented cloud accreditation scheme [64]. FedRAMP is the Government framework used for standardising security assessment and authorisation to assess and examine the security of cloud service providers. Once cloud service providers obtain FedRAMP Accreditation, it provides opportunities to conduct business with the federal government for use many times. In other words, any cloud service providers listed in the marketplace have compliance with the Government's security requirements, and the US government recognises them as authorise cloud providers.

Another example is the UK G-Cloud programme [89]. The G-Cloud framework has anticipated that accredited cloud service providers listed in the Government Digital Marketplace can deal with most official information. Cloud service providers that want to provide service to the UK government are necessary to get accreditation according to G-Cloud Information Assurance Requirements and Guidance. Three types of service are defined, namely: unassured cloud services; assured public cloud services; and formally accredited public cloud or private cloud services. Each service is intended for different types of information and business processes. For example, in this accreditation scheme, only accredited public cloud or private cloud services can handle most official information. Thus, cloud service providers that are accredited by the framework have opportunities to conduct business with the UK government and public sector organisations.

2.4.6 Service Level Agreement

Another type of assurance systems is Service Level Agreements (SLAs). An SLA is a formal definition of a relationship that exists between a service provider and a customer, defining agreed levels of services in the form of qualitative and quantitative terms as well as responsibilities of both parties [90]. The applications of SLAs as trust enhancing instruments are to establish a written contract between a customer and a service provider regulating their interactions and formulating their agreement regarding both functional and nonfunctional

requirements. In other words, an SLA can serve as a binding agreement between service providers and customers to establish the obligation of service providers to deliver service capabilities (e.g. security capabilities) according to service requirements (e.g. security requirements) elicited from customers [33, 50].

However, the term of SLAs and contracts have distinct meaning and are used interchangeably. A contract is a legal document between parties written by lawyers while an SLA is a service agreement between a service provider and a customer to specify the specification and level of service provided according to customers' expectation and service providers' resources [33]. In other words, an SLA is a type of contract which focuses on agreed service metrics that regularly monitored, updated, and improved according to customers' requirements and service providers' capabilities. In practice, the SLA can be reviewed and revised to help ensure that the agreed levels of services represent the needs of the business without having to revise the contract.

In practice, some SLAs are contracts which can be legally binding and enforced. Sometimes non-contractual SLAs can provide the metrics that play essential roles for selecting external information system services, defining and enforcing service agreement, monitoring external services, and accountability and auditing [91]. For example, if there is no agreement between parties to agree with some aspects of service, it is not an 'SLA', but simply 'contract'. However, both contracts and SLAs are legally binding. Thus, SLAs can serve as a means of defining the level of service in qualitative and quantitative terms while contracts are legal documents between parties.

There has been significant growth in the use of SLAs in service-based environments, such as cloud computing. An SLA is an effective means to measure technical services and manage business relationships between parties [92]. The reason behind the use of SLAs is to examine the service provider's capabilities to meet the customer's requirements and to agree on levels of expectation between parties [93]. In other words, the application of SLAs consists of the minimum acceptable service level which is determined by the consideration of the service provider's capabilities and the customer's requirements.

Further, the use of SLAs can serve as a means of expecting and managing mechanisms for achieving shared expectations about services and deliveries [94]. An SLA is essential as a

communication tool for business relationships between service providers and customers [94]. In such interactions, an SLA is paramount in setting a minimum acceptable level of service for both parties. Therefore, both parties should review their SLAs regularly for adaptation and change according to new requirements and situations. In other words, the development of SLA metrics should in line with customer's requirements and service provider's capabilities as the foundations for customers to trust in their service providers.

Based on such definitions, it is clear that SLAs can serve as instruments of customer control in the service scenarios [80]. The use of SLAs should be considered flexible and negotiated to suit the specification of new requirements and capabilities. The main reason for implementing the concept of assurance-based SLAs is to define and focus on the agreed service levels to meet customers' requirements. SLAs can describe delivered services and the lines of responsibilities, including robust auditing and monitoring capability for the customer [80, 81]. Additionally, SLAs can specify the characteristics of the services provided to customers in more precisely according to the customer's requirements and service provider's capabilities.

Hence it can be concluded that, although certification schemes are essential and widely used for assuring the security of information system services provided by service providers [27], the certification schemes are not well-suited to the service provisioning environment because the context of certification services does not apply for a dynamic threat environment [24]. Therefore, this thesis is concerned with SLAs as an assurance approach in a service provisioning environment. The following section discusses why SLAs are particularly relevant to government context and provide contemporary thinking on security-related SLAs.

2.5 Why are SLAs relevant to Government Context?

Many governments use external computing, communications and storage services offered by services provider to process, store or transmit government data to increase scalability and decrease costs of maintaining services [95]. Such external services usually are obtained through government procurements [13, 47]. Business relationships with external service providers are usually established through various instruments such as non-disclosure agree-

ments (NDAs), certification schemes and SLAs. However, NDAs and certification schemes are not well-suited to the service provision [24] while SLAs can serve as instruments of customer control in the service provisioning environment [80]. The application of SLAs is widespread when using external information system services, but there appears to be a gap of incorporating data confidentiality requirements into SLAs between government agencies and services providers when using such external services to process, transmit or store sensitive government data.

Indonesia is an interesting case study, as an emerging economy with a gross domestic product (GDP) around IDR 9.084 trillion [14]. The Government has used *e-Government procurement systems* for procuring information technology products, software and services since 2010, as set out in the Presidential Regulation Number 54 of 2010 on the procurement of government goods and services. Further, since the Government issued the Presidential Regulation Number 4 of 2015 in place of the 2010 regulation, the Government requires government agencies, including local government agencies to make use of electronic procurement system of which the procurement process is mandatory through an electronic procurement unit.

As stated in the Presidential Regulation No 4 in 2015, there are three types of electronic government procurement in Indonesia, namely: electronic tendering; electronic catalogue; and electronic purchasing. E-tendering is a process for selecting suppliers, conducted online and opened for all providers of goods or services registered on electronic procurement systems. E-catalogue is an online catalogue that contains information about products, including price and technical specification details. E-purchasing is a process for purchasing goods and services through the e-catalogue system.

Furthermore, the procurement of government goods and services can be conducted through a self-managed process or a third party. There are four electronic procurement models, namely: a government-owned and -operated service; a government-managed service; a public-private partnership; and a shared service model. However, the fact that there are limited security requirements applied to select service providers that provide external information system services to many government agencies in Indonesia.

This study focuses on e-tendering for selecting service providers through the public tenders (contract value more than IDR 5 billion) and the simple tenders (contract value maximum IDR 5 billion). This study examines central government agencies who want to procure external information system services, such as Internet services, data centre services and cloud-based services from external service providers. In other words, this study focuses on either a government managed service or a shared service model.

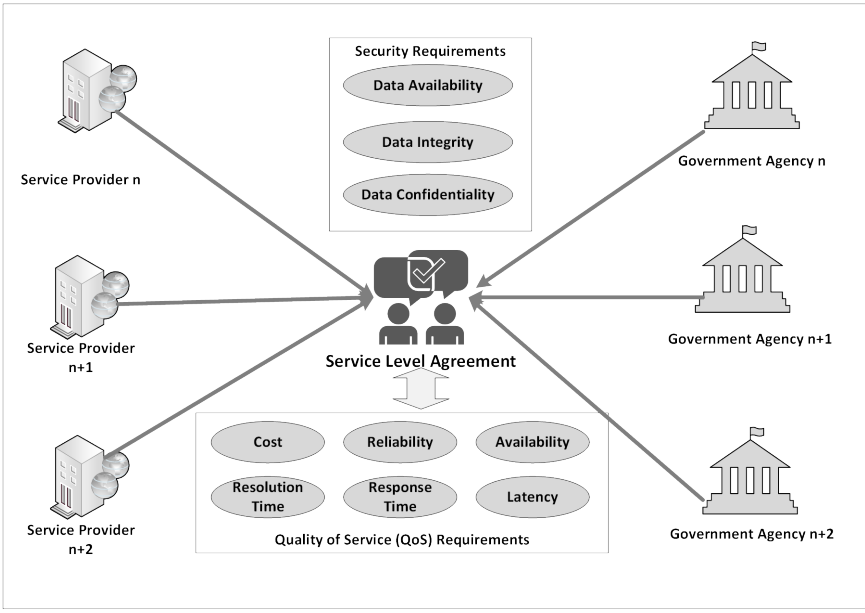


Figure 2.2: A Perception of Service Level Agreements (SLAs)

In particular, under Article 12, paragraph 1 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, all service providers that operate in Indonesia have obligations to have agreements on service level and security when providing such information technology services [13]. The provision of such regulation inherently implies that service providers who offer external system services are required to provide security service level agreements (security-related SLAs). In the following (Article 15, paragraph 1), service providers are also required to preserve the confidentiality, integrity, and availability of personal data, including citizen's data that is processed, stored or transmitted in the information systems. However, since uncertainties in the implementation of such provisions, there is no relationship between the application of SLAs with an appropriate level of security for services.

Further, the current provisions of SLAs focus on the system availability and performance aspects, without considering security aspects [33, 34, 96]. Such SLAs also include quality of service attributes (e.g. throughput, response times, resolution times and service availability), as shown in Figure 2.2. The incorporation of security requirements (considering data confidentiality) is difficult, especially when expressing such attributes in SLAs [33, 34] because of the lack of linkage between the level of security and SLA attributes. Debate continues about the appropriate assurance approach in a service provisioning environment. So far, the use of assurance-based SLAs is becoming increasingly crucial in procuring and using such external information system services that handle sensitive government data.

2.6 Security-related SLAs

The term *security property* is widely used in information security literature (i.e. confidentiality, integrity and availability). In addition to this, according to ITU-T Rec. X.805 [97], security properties can include access control, authentication, non-repudiation, communication security and privacy. The formulation of security properties (i.e. data confidentiality, data integrity and data availability) has not been expressed in such measurable terms in SLA contexts because security is a process and not a product [70].

According to Chan et al. [98], such security properties (i.e. availability, data confidentiality, data integrity, access control, authentication, non-repudiation, communication security and privacy) can be used as security SLA attributes. From a security perspective, availability is intended to ensure that there is no denial of authorised access to network and service elements. For example, the authors propose a percentage of downtime due to security incidents as feasible metrics [98]. Although Chan et al. [98] argue that data confidentiality and integrity are the primary security properties that can serve as security SLA attributes, there is a little knowledge how to define metrics or level of assurance for data confidentiality and integrity, which can be understood and accepted by customers and service providers [99]. The rest of such security properties does not receive the same degree of attention as the system availability of which metrics are not well-established. It appears that few studies have developed metrics for such security properties.

The first notion of security-related SLAs is proposed by Henning [31], who presents security-related SLAs as a mechanism to specify security services required for security policy enforcement. Due to the lack of quantifiable security attributes, such property does not exist in such measurable terms in SLA contexts. Moreover, the author underlines that it is challenging to include the costs of security services in SLA contexts. The author concludes that expressing security considerations in SLAs remains a significant need for more research.

Monahan and Yearworthy [32] support the previous argument. The authors state that statistical attributes need to be accepted by both the customer and service provider to develop adequate security-related SLAs. The authors investigate the problem of formulating an appropriate SLA for the use of anti-virus services. Moreover, the authors argue that security-related SLAs are necessary as value-added security services. Thus, the same approach taken in formulating anti-virus services can be applied to other security-related SLAs, such as patch management, security incident management and secure data transfer endpoints within an internal network.

Similarly, Bernsmed et al. [33] point out that the incorporation of security properties into explicit agreements or SLAs is essential. The authors argue that the deficiency of security properties in SLAs makes it not suitable for service providers to deliver trustworthy services to customers, especially when service providers and other suppliers are involved in delivering such services. However, the authors identify that there are still many questions about the formulation and adoption of such security-related SLAs in the context of service provisioning. For instance, security requirements may conflict with other quality of service requirements in SLA contexts.

In the same vein, Jaatun et al. [34] state that security-related SLAs are essential for external information system services to help ensure that service providers and customers have a shared perception of security attributes incorporated into SLA contexts for which customers receive the required level of assurance. Additionally, the authors reveal that many service providers provide quality of service as part of their contracts. However, the absence of assurance levels for data confidentiality, integrity and availability is problematic from the customers' perspective. Therefore, the authors suggest that the formulation of

security mechanisms in contracts or SLA contexts is paramount of importance. However, the authors emphasise that formulating security-related SLAs are not adequate if the agreed terms cannot be monitored and measured.

Furthermore, Takahashi et al. [35] present security-related SLAs which define the security level of service agreed between the customer and service provider. The authors point out that the formulation of security-related SLAs is built through matching and negotiating the customer's security requirements and the provider's security capabilities. Moreover, the authors argue that security controls according to perceived risks are required to be defined in terms of several variables in SLA contexts. However, the authors point out that such security requirements and capabilities may change dynamically depending on a threat environment.

Lee et al. [36] propose ontologies for security-related SLAs to understand the security agreements of a service provider and negotiate the desired security levels between contracting parties. Such ontologies aim to help comply with audit and compliance requirements for applicable laws and regulations, such as Health Insurance Portability and Accountability Act (HIPPA). The authors argue that understanding security-related SLAs offered by cloud service providers are necessary for customers to decide whether to procure cloud-based services for processing, storing and transmitting such sensitive data. However, the authors point out that existing ontology-based cloud SLAs provided by service providers is difficult to understand, thus comparing such SLAs from different service providers can also be challenging to manage.

Moreover, Luna et al. in [37] identify the absence of a straightforward approach to quantify security requirements in SLA contexts. The authors underline that it is challenging to understand what security levels customers have been paying for when using cloud-based services. Moreover, the authors argue that the elicitation of security requirements is essential to provide an appropriate security level to meet customers' needs. Therefore, the authors propose an approach to assess security level quantitatively and to enable customers to differentiate between other service providers. In other words, the proposed approach allows both novice and expert customers to express their security requirements according to security levels provided by cloud service providers.

Similarly, Guesmi and Clemente in [38] emphasise that service providers should be able to express what they can provide about security capabilities specified in SLA contexts according to security requirements. It helps ensure service providers are compliant with security requirements. However, the authors point out that that existing cloud service providers do not adequately express security properties in SLAs. Therefore, the authors introduce an approach called *a general requirement specification language* in which customers can express their security requirements regarding access controls and security properties, while the cloud service providers can express their related security capabilities.

Several consortia have proposed frameworks for expressing security-related SLAs in a cloud computing environment [100, 101]. For example, the secure provisioning of cloud services based on SLA management (SPECS) is developed to provide security-as-a-service, by expressing the notion of security framework in SLA contexts [28]. Similarly, the multi-cloud secure applications (MUSA) framework is developed to support the security-intelligent lifecycle management of distributed multi-could applications [29]. Likewise, SLA-Ready is proposed to support a reference model for developing cloud SLAs [30].

Furthermore, such frameworks support service provision for confidentiality considerations. For example, MUSA provides techniques for ensuring data confidentiality, data integrity, data protection, data privacy requirements are satisfied in multi-cloud applications [102]. Similarly, SPECS also offers end-to-end encryption mechanisms through existing security controls. Whereas, SLA-ready considers use cases requiring data security and key management for expressing the service level objective requirements [102]. However, it seems that those frameworks still do not adequately address the question of incorporating the Government's data confidentiality requirements into SLAs according to the data classification and threat model. The importance of SLA-based discrete security assurance levels is still not adequately considered when using external information system services which are processing, transmitting and storing sensitive government data.

2.7 Gap Analysis

Based on the latest thinking on security-related SLAs as discussed above, this section provides a gap analysis that motivates the research undertaken in this thesis.

The literature review presented thus far provides evidence that there are a growing awareness and application of security-related SLAs in practice. The formulation of security-related SLAs in the service scenario is acknowledged to be an essential foundation of assurance. Several attempts have been made to express security properties in SLA contexts. However, it seems that the literature still lacks insights into the question of incorporating the Government's data confidentiality requirements into SLAs according to the data classification and threat model.

Furthermore, the issue has grown in importance after the secret documents made public by Edward Snowden particularly about the NSA's PRISM surveillance program [103] in which many governments doubt the policy of procuring external information system services like cloud-based services, which are primarily supplied by the US companies. The importance of SLA-based discrete levels of assurance is still not adequately considered when service providers are handling sensitive government data and assets.

Although extensive research has been carried out on security-related SLAs, there appears to be a gap which adequately covers empirical studies on investigating government's data confidentiality requirements in SLA contexts. Recent contracts and SLAs are found to make use of security controls like NIST 800-53 and ISO/IEC 27002 [28, 30]. In other words, incorporating existing security controls into SLAs constitutes security-related SLAs. However, apart from the practical approach this presents, the inclusion of security controls in the SLA contexts do not achieve a specified level of security assurance, but instead, only provide a binary assurance (compliant or non-compliant).

Therefore a research opportunity exists to advance the state-of-the-art by elaborating and formulating such security controls to discriminating levels of security assurance which is of utmost significance for incorporating the Indonesian Governments' data confidentiality requirements into SLAs between government agencies and service providers. Due to the lack of understanding of the concept of system assurance and trustworthiness, especially when

government agencies procure and use external information system services from service providers, this thesis seeks to fill this gap and present principles as foundations for a TDSLA capability framework. The original inspiration for building a TDSLA capability framework is the CC certification process. CC aims to certify levels of security for products while the TDSLA capability framework aims to certify levels of security for services.

To this end, this thesis conducts socio-technical qualitative research by collecting and analysing data from three empirical studies in which each conducted with different settings and participant groups, using Indonesia as a case study. This thesis anticipates that the concept of a TDSLA capability framework can be used to provide benefits in contexts beyond the Indonesian Government. The work on the Government's data confidentiality requirements serves as the context of empirical data collection to support the investigation, development and evaluation of foundations for a TDSLA capability framework.

2.8 Choice of Research Methods

This thesis proposes principles as foundations for a TDSLA capability framework between government agencies and service providers, using Indonesia as a case study. To this end, this thesis investigates three exploratory qualitative studies through adaptive wideband Delphi with Indonesian participants, with group discussion and individual session [14]. Each conducted with different settings and participant groups.

A qualitative method using grounded theory analysis was chosen to propose principles as foundations for the proposed framework [104]. In this study, the application of grounded theory aims to generate principles and framework rather than use or validate existing framework [105]. The grounded theory approach has become a well-established research methodology by which new frameworks can be uncovered, by process of data collection activities, coding and categorisation, followed by several comparative and theoretical analyses of findings [106–111].

Due to the lack of previous studies on the concept of security assurance-based SLAs in a government scenario study, this thesis develops principles as foundations for a TDSLA capability framework between government agencies and service providers. Data collection

from three empirical studies was analysed, which involved identifying categories and relationships among categories. Therefore, the chosen grounded theory approach is used to develop principles and uncover the contextual categories of a TDSLA capability framework.

Using grounded theory has the advantage of being a systematic but flexible approach to analysing qualitative data. Additionally, this method can analyse complex social phenomena and experiences [108, 109]. Consequently, the grounded theory is a practical approach to develop principles and framework from the empirical data. However, using the grounded theory approach has limitations, such as the researcher might be biased, a misinterpretation of coding procedures, and single case study with limited participants. Some steps have been taken to minimise the influence of these limitations. Despite the limitations of the research method, grounded theory is a suitable technique to present principles as foundations for a TDSLA capability framework because of an iterative development process.

2.9 Chapter Summary

This chapter has provided background about the major components that are relevant to the notions of trust and trustworthiness in the context of a service provisioning environment where SLAs can serve as critical elements defining trust between government agencies and service providers. The concept of assurance-based SLAs with discrete levels of security assurance is introduced to address the problem of security evaluation in service provision settings. Compared to the concept of security assurance-based certifications (e.g. CC and ISO/IEC 27001), the security assurance-based SLA metrics is appropriate to support a dynamic service environment, such as cloud-based services.

This situation contrasts with well-established norms for systems such as the CC framework, which is essential as the basis for a government-driven certification scheme and security evaluation for information technology products and systems. However, applying security assurance-based CC is an expensive process and known to be slow moving to pass the evaluation. CC seems valid only within the scope of a protection profile that is the subject of a security evaluation under the CC certification.

However, the fundamental inspiration and reference point for building a TDSLA capability framework is the CC certification process. CC aids to build trust through two main components, namely: protection profiles; and evaluation assurance levels (EALs). A protection profile specifies a set of security requirements for a specific type of product. Unlike protection profiles, the EAL does not show the actual security capabilities of the product, but independently evaluates the product as evidence of adequate testing against the security target. The security target description covers an overview of the product, potential security threats and any claims of conformity against a protection profile at a specified EAL.

In the same vein, developing foundations for a TDSLA capability framework consists of two main components, namely: discrete assurance levels; and service level agreements. A discrete level of assurance defines a standard set of data security requirements for a specific type of threats and data classification level. The technical, procedural and human controls of information security are essential to achieving the required level of assurance. Each level of assurance is distinct from another, depending on a type of threats and data classification level. In addition to discrete assurance levels, the use of service level agreements is intended to examine a service provider's capabilities to meet the customer's data security requirements and to agree with the required and provided a level of security assurance between parties.

Therefore, these are the reasons to construct better assurance mechanisms in service provision that give government agencies as much transparency and confidence as possible that any sensitive government data transferred to service providers is processed, stored or transmitted securely against unauthorised access. In other words, the CC aims to certify levels of security for products while the TDSLA capability framework aims to certify levels of security for services. Proposing principles as foundations for a TDSLA capability framework is presented in Chapter 7, draws from three qualitative studies (presented in Chapters 4, 5 and 6) that incorporate views of 50 participants from the Government and service providers.

3
Methodology

> *Not everything that can be counted counts, and not everything that counts can be counted*
>
> Albert Einstein,

Chapter 3 partially draws on refereed article described in the following publication:

- Y. Nugraha, I. Brown and A. S. Sastrosubroto. "An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements". In: *IEEE Transactions on Emerging Topics in Computing*. vol. 4. no. 1. pp. 47-59. 2016 [14].

Contents

3.1 Introduction

Real-world qualitative empirical studies pose many challenges. In this study, the investigation of the Government's confidentiality requirements was challenged by the need to gain access to knowledgeable respondents. When it comes to discussions about the government's security posture, few government participants, including government consultants and service providers, are willing to share their experiences. To this end, this chapter introduces and justifies the choice of the methodology used to investigate the problem of incorporating the Government's data confidentiality requirements when using external information system services supplied by external service providers.

This thesis reports on three empirical qualitative studies using Indonesia as a case study to guide the development of foundations for a TDSLA capability framework. These qualitative studies are conducted through an adaptive Delphi study, grounded theory, and a combination of the Delphi method and grounded theory called the grounded adaptive Delphi method (GADM).

As mentioned in the previous chapter, each empirical study has different settings and participant groups. Chapter 4 conducts a qualitative empirical study of the Indonesian Government's security needs to mitigate unauthorised access, especially posed by global adversaries, (e.g. foreign intelligence services), using an adaptive Delphi study. Chapter 5 investigates an understanding of government SLA data confidentiality requirements from the Indonesian government participants. Chapter 6 examines an understanding of service provision for confidentiality in SLAs among service providers that offer external information system services to Indonesian government agencies. These two chapters use the GADM approach to address such research questions.

Furthermore, Chapter 7 goes on to propose principles as foundations for a TDSLA capability framework between government agencies and service providers. It does this by conducting a qualitative analysis using a grounded theory approach of two previous empirical qualitative studies (Chapter 5 and Chapter 6). The research design developed for this research represents a significant contribution that this thesis makes.

In this chapter, Section 3.2 provides background information related to the philosophical foundation of qualitative research. The subsequent sections (Sections 3.3 - 3.5) describes the details of the methodology used in this thesis. Section 3.6 discusses approaches for validating grounded theory results. The final section concludes a summary of this chapter.

3.2 Research Philosophy

This thesis undertakes research, to investigate the inclusion of the Government's data confidentiality requirements expressed in the form of SLAs, by using data from the field. The choice of qualitative study reflects the nature of the problem, which relates to understanding social phenomena in the context of addressing security within supplier agreements.

Morse [112] considers qualitative methods when a topic is little known, and the research context is poorly understood. At this point, researchers consider such methods when the boundaries of the domain are unclear, and the phenomena are not quantifiable. Moreover, qualitative research is the best option when the nature of the problem is not clear. Similarly, Bricki and Green [113] point out that it is often better to start with qualitative methods using interviews or focus group discussions if such a problem is unknown. In general, qualitative methods aim to answer questions about the '*what*', '*how*' or '*why*' of a phenomenon rather than '*how many*' or '*how much*', which are answered by quantitative methods.

Qualitative research involves employing multiple data-collecting methods, especially using participant interviews and focus groups. It uses an inductive approach to analyse data by extracting categories and themes from collected data which constitute an understanding of the context. There are several methods for conducting qualitative research, namely case studies, grounded theory, ethnography, content analysis and phenomenology [39, 40]. If the purpose is to construct principles or a theoretical framework that reflects reality rather than from a researcher's perspective or previous studies, such research methods like grounded theory can assist the discovery of theory from the data [43]. There are, however, limitations of data collection in qualitative research, such as it may be labour and time-consuming. There are also challenges in establishing generalisability of the research beyond the specific case that is being investigated.

This thesis uses the case of Indonesia to conduct three extensive qualitative studies served as evidence for developing foundations, using an adaptive Delphi method, grounded theory and the GADM approach. The following sections provide an overview of both the Delphi method and grounded theory, which constitute various elements that form GADM.

3.3 Adaptive Delphi Method

The RAND Corporation developed the Delphi method in the 1950s as part of a military defence project [114, 115]. This method moderates the influence of dominant individuals and follows a rigorous sequence of steps for decision making in the context of policy formulation [114]. All features of the Delphi method, such as anonymity, iteration and controlled feedback and statistical group response, are used to elicit and refine group estimation and consensus [114, 115]. This approach avoids direct conflict among participating participants due to the absence of face-to-face communication [116].

Many researchers have adapted the Delphi method for use in specific situations [116], as shown in Table 3.1. For example, participants can partake in a Delphi study by connecting via a custom website [117] or email [115].

Table 3.1: Variants of the Delphi Method

Variant	Variance	Reference
Policy Delphi	Establish differing positions instead of consensus	Turoff (1970) [118]
Modified Delphi	Close questions	Kerlinger (1973) [119]
Wideband Delphi	Discussion among experts prior to submission of individual responses	Boehm (1981) [25]
Ranking Delphi	A brainstorming session, select, and rank	Dickson et al.(1984) [120]
EFTE: An interactive Delphi method	Committee-like discussion following the study	Nelms and Porter (1985) [121]
Real-time Delphi	Immediate availability of responses to all	Gordon and Pease (2006) [117]

Of specific relevance to this thesis, the Wideband Delphi method involves a higher level of interaction among participants than the classic Delphi method [122]. Group discussions

between rounds are allowed in which participants can illuminate and explain their statements and opinions [25]. While traditional Delphi studies avoid face-to-face meetings to elicit anonymous input, the Wideband Delphi estimation can help to clarify the major issues when 'judgmental information is indispensable' [116], and to seek all requirements as 'informed judgement' [123]. This iterative process terminates when none of the participants wants to revise the joint estimation [124].

However, there are particular problems with the use of the Delphi method. Such a method assumes that securing participants to participate in face-to-face meetings, is straightforward - which it was not. This barrier was primarily the experience when working with *elite* participants, such as government experts. Furthermore, it is essential for participants to understand and acknowledge the importance of the research objectives. Therefore, it is necessary for participants to have a clear understanding of the problem description and the Delphi steps before the study begins.

With this understanding, the thesis develops an adaptive Delphi method based on the traditional Delphi method and the Wideband Delphi method in order to best engage with such participants as well as minimise barriers to completing the data collection activities. This method appears as a practical way to investigate government's confidentiality requirements by using Delphi features, such as anonymous individual feedback, controlled feedback and group responses with face-to-face meetings [14].

3.3.1 Participant Selection

The selection of participants is a critical aspect of a Delphi study [125]. Fundamental to Delphi studies is the understanding that group decision has great validity than those of a single person [126]. These decisions are trustworthy only if participants are knowledgeable about the research topics [126]. It is for this reason that Hsu and Sandford [125] suggest that researchers must select participants according to their expertise with specific issues.

Since the motivations and experiences of participants directly affect the quality of the findings, selection criteria are necessary to ensure appropriate participants contribute to study findings. Rowe et al. [127] suggest the following criteria: ease of availability; reputation;

and expertise related to the research problem. Each of three empirical qualitative studies discusses participant selection in more detail.

Regarding the number of participants, there is no consensus about the optimum number of participants required for a successful Delphi study [125]. Even so, a Delphi study requires many participants to obtain divergent opinions [128]. For example, Okoli and Pawlowski [116] have recommended 10–18 participants in a Delphi group. According to the literature, the recommended number of participants varies between 5–20 people [129], 10–15 people [130] and 15–20 people [125].

This thesis engages with 70 participants over three empirical studies. Each is conducted using various settings and participant groups (e.g. the Government and service provider participants). Each Delphi round had between 6-35 participants. While 12 interviews are considered necessary to gain a comprehensive set of data, it is still possible to discover basic meta-themes after six interviews [131]. Therefore, the instance of a small number of participants was still considered sufficient for providing a reliable analysis.

3.3.2 Data Collection

Many researchers suggest a two-round of Delphi study, with generally three rounds for data collection activities [128, 132, 133]. In practice, the first round of a Delphi study is a brainstorming phase, and the following subsequent round is an enrichment phase for discussion of results obtained in the previous round [14]. The third round is an integration phase to combine categories that are similar in essence, as shown in Figure 3.1.

3.3.2.1 Group Interviews (Focus Groups)

In the first round, a Delphi study begins with an exploratory stance, which elicits participants' thoughts and opinions regarding a specific problem. This round can be conducted as a brainstorming session asking participants to identify and discover varying opinions of the problem. Thus, this phase can be carried out in the form of a focus group discussion.

A focus group is a group discussion on a specific topic conducted for research purposes [134]. A focus group provides some advantages over interviews, especially where

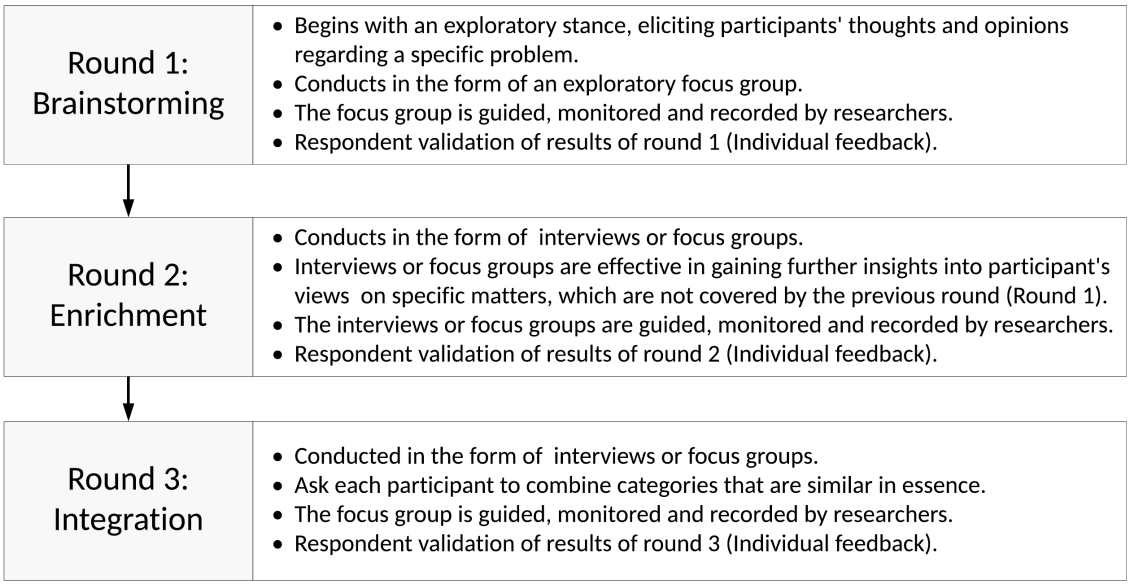


Figure 3.1: A Three-Round Delphi Study

individual participants may have difficulty expressing their ideas on a particular subject. This phase aims to seek exhaustive information on collective views [134] or to generate a rich understanding of participants' opinions. In this point, researchers play a role in controlling and overseeing focus group activities [135].

One of the significant advantages of using focus groups is that it allows researchers to explore topics, gather ideas and collect feedback from participants for use in the later stages of a study. Another benefit of the focus groups is that it allows researchers to present feedback or results to participants [134, 135]. However, the focus groups can lead to the phenomena of groupthink in which a group of participants makes decisions because some of them do not want to express contrary opinions [134, 135]. As such, the research method used in this study attempts to counter groupthink by eliciting opinions from individual interviews.

The participant number is an essential consideration in focus groups. Although there is no consensus view for the ideal composition of the group, Gill et al. [134] suggest that the optimum focus group size is between six to eight participants (excluding the moderator). However, such a focus group can work successfully with three to fourteen participants [134]. In this thesis, the group size varied between three participants to fourteen participants in response to participant work schedules.

3.3.2.2 Individual Interviews (Interviews)

For the second and later rounds, data collection can be conducted either through interviews or focus groups to gain a deeper understanding of participants' experiences and opinions, based on the results of the previous round. Furthermore, individual interviews aim to explore the genuine opinions of each participant on specific questions to provide a thorough understanding of the target issues. Interviews are an appropriate method for exploring sensitive topics where participants may not wish to elaborate in a group discussion [134]. Such an approach allows participants to express any other information about the research questions [134, 135].

3.4 Grounded Theory

Grounded theory (GT) is a well-established qualitative research method to generate theory from the data rather than to test or validate an existing theory [2, 136]. GT is a rigorous approach, as it outlines a series of research activities regarding how to collect and analyse data [108, 137]. Since the goal of GT is to develop a theory from the data [136], the grounded theory is an appropriate method for investigating areas or situations where little is known, such as in exploratory or discovery - oriented research [112, 113, 138].

GT has been making in-roads into engineering and computing research. For example, GT is very well-known in software engineering [2], human-computer interaction and computer-supported cooperative work [137]. Additionally, GT studies in cybersecurity and privacy have been growing. For instance, the use of GT as a methodology has appeared at flagship security conferences, such as the USENIX Security Symposium [106] and the ACM CCS Conference [107]. Moreover, several peer-reviewed technical journals, including Computers and Security Journal [109] and Proceeding on Privacy Enhancing Technologies [139] have published such grounded theory studies.

The primary research process of GT consists of collecting, coding, conceptualising and categorising the data, following by specifying the relationship between the categories to integrate them into a cohesive theory [108]. Different versions of GT lend themselves to various coding procedures [2]. For instance, Glaserian GT [136] introduces coding meth-

ods, namely open coding, selective coding and theoretical coding procedures. Straussian GT [140] employs open, axial and selective data coding. While Charmaz's Constructivist GT [108] consists of initial coding, followed by focused coding and theoretical coding, as shown in Figure 3.2.

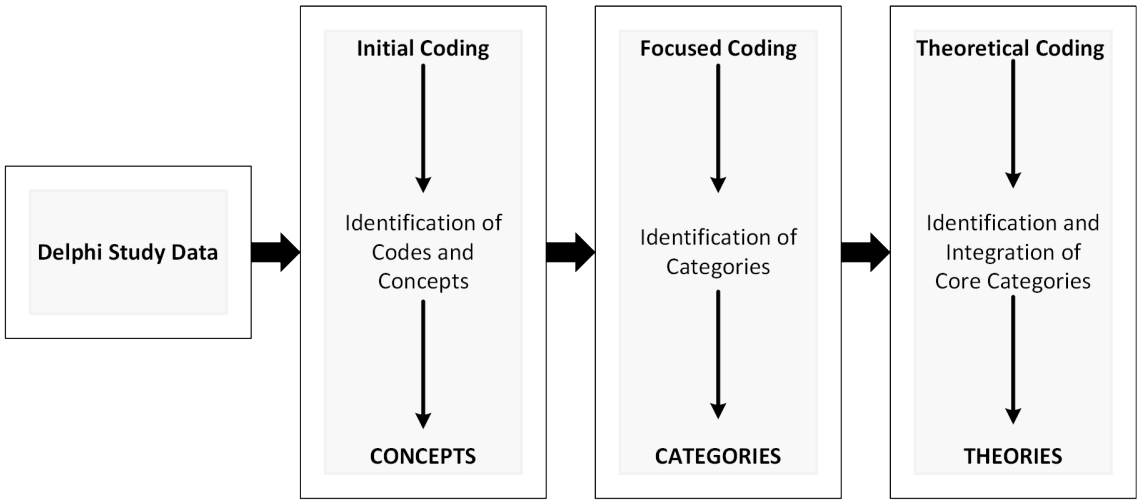


Figure 3.2: A Grounded Theory Analysis

The methodology used in this study is an instance of a grounded theory analysis. This research uses coding procedures, namely initial coding, focused coding and theoretical coding [108] to facilitate data analysis in the Delphi study data. The following discusses in more detail the nature of GT analysis.

3.4.1 Initial Coding

The first step in GT analysis is an initial coding of the data. This initial coding process is similar to the idea of open coding as seen in Glaserian GT and Straussian GT. The initial coding process breaks the data into concepts by examining interview or focus group transcripts, through word-by-word, line-by-line, incident-by-incident, by sentence or paragraph or even by the whole documents [2, 108]. Such a process extracts useful sentences or statements, and identifies topics of interest, called 'key-point coding'. Organising these initial codes into more complex conceptual codes occurs in focused coding, as shown in Table 3.2.

Table 3.2: Examples of the coded data that emerged from the data

Data/incident (Translation)	Code/concept	Category
'if we look at the present state, almost all cases of data leaks occur because of an insider, whether committed by an employee or a former employee'	identifying insider threats by employees	collaborator
'*regarding the most sensitive government data, the issue of sensitive government data theft normally does not occur while data is transmitted, but when data was processed or created. While discussing with, an insider can listen and participate in the discussions and then disclose and share the information obtained with an adversary*'	identifying insider threats by employees	collaborator
'*There is a threat, which we consider before the threat was always from the outside, so we then place a firewall, intrusion detection, and so forth. But the fact that now the threats and attacks actually come from inside. According to our observation, we discovered botnets keep sending out information*'	identifying outbound traffic	exfiltration
'*when we communicate, we must remain aware of our level of communications, whether or not it is important in relation to confidentiality of information transmitted...we are aware that when we are talking with our interlocutor, there must be other people listening without knowing them*'	identifying interception	observation
'*they embed code on the opposing side in any way to divulge the sensitive government data*'	identifying malware injection	insertion
'*For threats to military information and sensitive government data, in general, the threats were in the form of impersonation. Besides the impersonation, they can also do phishing*'	identifying a ransomware installation	manipulation

3.4.2 Focused Coding

Focused coding follows on from initial coding. This coding process is similar to selective coding, based on Glaserian GT [136], which focuses on generating codes around identified core variables [2]. The focus coding process is similar to the axial coding step described in Straussian GT [140], which involves the identification of relationships between categories and subcategories and to each other before being tested against the data [2].

In Charmaz's GT [108], the focused coding process allows researchers to select categories from the most common or essential codes [2]. In other words, this coding process begins to select categories from amongst topics of interest and finds relationships among these initial codes (e.g. the most frequent or important codes) [108, 140].

3.4.3 Theoretical Coding

Theoretical coding is at the heart of theory development or theoretical integration [108, 141]. In Glaserian GT [136], the theoretical coding aims to identify the conceptual relationships between the substantive codes, thus informing the development of a hypothesis [2]. Similarly,

Straussian GT [140] discusses a theoretical integration within the process of selective coding, which aims to identify a core category that links all significant categories [2]. Although Straussian GT [140] is required to determine a central category, the Charmaz's GT does not need the choice of core concepts [108], as shown in Table 3.3.

Once the categories are identified, this step establishes the relationship between the categories to integrate them into a cohesive theory [108]. Overall, this thesis uses GT primarily for data analysis. The outcomes of the GT analysis are elements of the proposed principles or a framework.

Table 3.3: Differences between the three main strands of GT [2]

Element	Glaserian GT	Straussian GT	Constructivist GT
Research Question (RQ)	RQ should not be defined a priori, but emerge from the research.	RQ may be defined upfront and derived from the literature.	RQ begins with 'initial research questions' which evolve throughout the study [108].
Role of the literature	An extensive literature review should be delayed after the theory is emerging to prevent the influence of existing concepts on the emerging theory.	The literature may be consulted throughout the process, as concepts from the literature may be used if applicable.	Charmaz [108] highlights the need to tailor a literature review to fit the purpose of the GT study.
Coding Procedures	**Open coding**: 'fracturing' of the data; line by line coding is recommended to achieve full theoretical coverage, but does not reject coding sentences or paragraphs, or whole documents [142].	**Open coding**: generation of 'categories' and how they vary dimensionally. Coding can be done a line-by-line or by sentence or paragraph, or even the whole document [140].	**Initial coding** is conducted by examining data word-by-word, line-by-line or incident-by-incident to make sense of the text without injecting the researcher's assumptions, biases, motivations.
	Selective coding: delimiting coding to only those variables that relate to one core variables to establish a parsimonious theory. The core variable guides further collection.	**Axial coding**: putting back data in new ways after open coding by identifying relationships between categories.	**Focused coding**: selecting categories from the most frequent or important codes and using them to categorise the data; does not require a single core category.
	Theoretical Coding: establishing conceptual relations between substantive codes, resulting in the development of hypotheses.	**Selective coding**: deciding on the central category that all major categories can link to [140].	**Theoretical coding**: specifying the relationship between categories to integrate them into a cohesive theory.
Evaluation Criteria	1) The generated categories must fit the data; 2) The theory should work; 3) The theory must have relevance to the action of the area; and 4) The theory must be modifiable as new data appear.	Seven evaluation criteria for the research process, such as sample selection, major categories and derived hypotheses. Eight criteria regarding empirical grounding such as concepts generated, many conceptual linkages and variation built into the theory.	1) Credibility (is there sufficient data to merit claims); 2) Originality (Do your categories offer new insights?); 3) Resonance (Does the GT make sense to participants); and 4) Usefulness (Does the GT offer useful interpretations?).

3.5 Grounded Adaptive Delphi Method (GADM)

The methodology adapted for this study combines elements of the Delphi method and GT. Both the Delphi method and GT consist of simultaneous data collection and analysis, with each process being interrelated and iterative [41]. The Delphi method aims to identify diverse opinions on specific questions as part of individual and group responses [124], whereas GT aims to develop a theory or framework from the Delphi study data.

The grounded adaptive Delphi method (GADM) is a new research method. However, several attempts have been made to develop such a method. For instance, Moe and Paivarinta deal with the challenges of information systems procurement in the Norwegian public sector [42]. Similarly, Howard [41] explores the skills, knowledge and education needs of information professionals in galleries, libraries, archives and museums (GLAM) in Australia.

Table 3.4: Grounded Adaptive Delphi Method (GADM)

Version	Participant Selection	Round 1: Brainstorming	Round 2: Enrichment	Round 3: Integration
Moe and Paivarinta [42]	Select expert panel	1.1: Brinstorming via email	2.1: Forming the consolidated list via ***open coding*** to identify concepts	3.1: ***Axial coding*** to suggest relationships
			2.2 Validating the consolidated list	3.2: ***Selective coding*** to confirm initial theory
			2.3 Analysis of Round 2 data via ***open coding*** to discover concept priorities	
			2.4 Norrowing down the list and rangking the challenges and using ***selective coding*** to discover core categories	
Howard [41]	Select expert panel	1.1 Brainstorming via sector-specific focus groups	2.1 Forming questionnaire (Round 2) via ***open coding*** to identify items	
			2.2 Validating the consolidated items	
			2.3 Analysis of Round 2 data via ***open, axial and selective coding***	
			2.4 Move towards consensus and determine if 'a priori'consensus level was met	
GADM	Select participants with snowballing sampling	1.1 Brainstorming via focus groups to seek information on collective views	2.1 Seeking a deeper understanding of participant's views or opinions on specific questions via focus groups or semi-structured interviews	3.1 An integration process using grounded theory analysis [106–108]
		1.2 Respondent validation of the focus group transcripts	2.2 Respondent validation of the focus group or interview transcripts	3.2 Respondent validation of the results of Grounded Theory analysis

This thesis employs the recently developed GADM, which varies in some respects from the two previous GDMs [41] and [42]. A significant similarity between such methods is the integration of GT analysis and the Delphi method with group discussions and interviews as a means of eliciting the opinions on specific problems. However, one of the differences is that the GADM approach used a *Policy Delphi* approach [118]. The objective of the Delphi method is not to achieve consensus but to explore diverse ideas, opinions, and views regarding a specific question, as well as to generate options for consideration [118]. Note that the adaptive Delphi method aims to suit the different views, opinions, thoughts, and experiences of individual participants on specific matters, with greater generalisability across various participants. The GT analysis is particularly well-suited for capturing these different views from participants in more detailed forms.

Another distinction is that the GADM approach combines elements of the Wideband Delphi method and the traditional Delphi approach, using group discussions and individual sessions [14]. The most significant difference with the previous studies in [41] [42] is that data collection is not conducted via email [42] or with an online questionnaire [41]. Such online questionnaires are impractical to elicit genuine opinions or thoughts from 'elite' participants, such as government participants. Instead, this study sought to engage with participants via focus groups and semi-structured interviews.

3.6 Evaluating Qualitative Research

Validity in research is concerned with the accuracy and trustworthiness of scientific findings [143]. The validity of quantitative research is well-developed, including internal validity, external validity and reliability. However, many qualitative researchers avoid the terms validity and reliability and use terms such as credibility, trustworthiness, truth, value, applicability, consistency and confirmability, when referring to qualitative research [142, 144].

Charmaz [108] notes that 'criteria for evaluating research depend on who form them and what purposes he or she invokes'. Such criteria for grounded theory studies include credibility (e.g. Is there sufficient data to merit claims?), originality (do your categories offer new insights), resonance (does the GT make sense to participants) and usefulness

(does the GT offer useful interpretations?), as shown in Table 3.3. However, criteria for adequate research may differ from various studies because the expectation for grounded theory studies may change [108].

Many qualitative researchers have proposed several approaches for validating grounded theory results [138,140,145,146]. *Triangulation* refers to the importance of gaining multiple sources and methods to check the results of grounded theory analysis whether different methods lead to the same result [138,145]. *Reflection against extant literature* [108,111,147] refers to comparing the extant literature with the data, codes, concepts, categories and theory during validation study. During this process, the data should be consistent before being compared with extant literature.

Furthermore, *testimonial validity* refers to the accuracy of the interpretations made by researchers [138, 144, 146]. Once a framework has been developed, it is the case that such researchers require access to participants to check whether such a framework is convincing to the participants. *Negative case analysis* describes the process of revising hypotheses as new negative cases arise [148, 149]. Similar to testimonial validity, such an approach requires access to participants after the analysis has taken place [138]. *Reflexivity* refers to the way researchers understand and acknowledge how their views change during data analysis because new data can adapt and change the theory [138, 146].

In [138,145], *thinking comparatively* is one such proposal. Strauss and Corbin emphasise the importance of such an approach to maintain objectivity by comparing incident to incident in the data. They also underline the importance of *theoretical sampling* in the context of constructing a theory from the data. Charmaz points out that the primary objective of theoretical sampling is to elaborate and refine the categories constituting a theory or framework [108]. Finally, presenting information about the context is essential for grounded theory studies because the results may apply only to the domain and context being studied [108]. Such context contains information about the transferability of the study to other settings and groups.

Overall, this thesis adapts some of the approaches taken in [111, 138, 146, 147] for validating grounded theory results, as follows:

1. **Testimonial Validity**—is the participant validation of focus group and interview transcripts during data collection activities. Once principles have been developed, participants will be asked for their feedback [146].

2. **Reflexive Validity**—is shown through the gradual refining of the analysis to encompass concepts, categories and theories that are grounded in, emerge from the data. A sample transcripts with the coding is presented in Appendix A [138, 146].

3. **Replication Validity**—refers to the applicability of findings from one context to another context. In other words, detailed information about the context is essential to provide information about the transferability of the study to other contexts [138, 146].

4. **Reflection against extant literature**—refers to comparing the extant literature with the data, codes, concepts, categories and theory during validation study [111, 147].

3.7 Chapter Summary

This chapter has provided a detailed discussion of the methodology used in this thesis, including the procedures used to collect and analyse data. The Delphi method and grounded theory have been discussed to explain the relationship between these approaches informing the GADM approach. This chapter has described the application of the GADM approach to this thesis. Furthermore, this chapter has provided justifications for the choices made about the methodology for this thesis. The following subsequent chapters employed such qualitative methods described in this chapter. Chapter 4 uses an adaptive Delphi method. Chapter 5 and Chapter 6 apply the GADM approach to address the research questions. Chapter 7 attempts to propose principles as foundations for a TDSLA capability framework between government agencies and service providers by conducting a grounded theory analysis of two empirical studies (Chapter 5 and Chapter 6). Overall, this chapter has developed specific research design and methodology for three qualitative empirical studies reported in this thesis.

4
Government Security Needs

> *Any discussion of computer security necessarily starts with a statement of requirements*
>
> U.S. DoD, *Trusted Computer System Evaluation Criteria*, 5200.28-STD

Chapter 4 draws on the refereed article described in the following publication:

- Y. Nugraha, I. Brown and A. S. Sastrosubroto. "An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements". In: *IEEE Transactions on Emerging Topics in Computing*. vol. 4. no. 1. pp. 47-59. 2016 [14].

Contents

4.1 Introduction

The secrets documents made public by a former NSA contractor Edward Snowden [9–12] have created unprecedented public awareness of alleged pervasive surveillance attacks posed by sophisticated and well-funded adversaries, such as foreign intelligence services, particularly to the Indonesian Government. Other governments, such as the Brazilian and German governments have responded to such threats by developing the government's security needs to protect sensitive government data and assets [55, 150]. These governments have been leading critics of the pervasive surveillance program posed by the US National Security Agency (NSA) and its foreign partners known as 'The Five Eyes Countries'.

The NSA documents revealed secret program about NSA's pervasive surveillance programs, such as PRISM [103], Tempora [151], Upstream [152], Phone Collection [153], Xkeyscore [154] and Stateroom [155]. Such threats can seriously harm the confidentiality of sensitive government data. Several studies [54, 55, 156, 157] have discussed possible proposals of mitigating such threats. For instance, many studies have suggested that local data clouds, data protection laws, decentralised Internet services, and investment in security professionals and intelligence experts are potential mitigation strategies to prevent unlawful processing by foreign intelligence services and global service providers [54, 55, 156, 157]. As such, it is important to consolidate reasonable efforts to mitigate pervasive surveillance attacks by developing an adequate defence-in depth-security.

Therefore, this chapter investigates the Indonesian Government's security needs to mitigate unauthorised access to sensitive government data, primarily in response to the case of Australian surveillance of Indonesia. To this end, this chapter develops and conducts an adaptive wideband Delphi method to gather statements from multiple stakeholders (government, military, industry, and government consultants) and analyses such statements to identify categories of security needs to protect sensitive government data across Indonesian government agencies.

Indonesia is an interesting case study as a non-aligned, large emerging economy with GDP around IDR 9.084 trillion (around USD 753.99 billion) [14]. Additionally, according to the Indonesian Internet Service Provider Association (APJII), Internet users in Indonesia

reached 139 million by 2015 [14]. In other words, a quarter of Indonesia's population is currently online. In particular, Indonesian is one of the countries that has been reportedly intercepted by the Australian intelligence agency.

Overall, this chapter identifies 25 categories of government security needs which are framed by the five defences-in-depth security elements: people, operations, technology, governance and legal remedies. Some security needs are correlated with the catalogue of security controls from ISO/IEC 27002 [66], NIST SP 800-53 [1], and 20 Critical Security Controls [158]. Other security needs identified are not related to any security controls listed in such standards.

The remainder of this chapter is structured as follows. Section 4.2 describes how to investigate government security needs, including participants' recruitment, procedure and data collection and analysis of findings. Section 4.3 presents the findings of the study. Section 4.4 discusses how the findings compare with related work and elaborate on the implications of the findings for concrete recommendations. Finally, Section 4.5 summarises the chapter.

4.2 Method

4.2.1 Aim

This chapter seeks to study the Indonesian Government's security needs to mitigate unauthorised access to sensitive government data (e.g. pervasive surveillance attacks), especially posed by global adversaries like foreign intelligence services. For this reason, this chapter develops and conducts an adaptive wideband Delphi method to elicit statements on participants' views concerning government security needs against unauthorised access. The participants of this study are elite participants from government, military, industry, and government consultants who have a significant influence on the conduct of the Government.

Furthermore, this chapter has adopted a threat-profile model [3] to describe and understand pervasive surveillance attacks, as described in Table 4.1. Additionally, adequate protection against threats requires the defence-in-depth approach to the protection of sensi-

tive government data. The defence in depth approach offers the ability to help mitigate such threats across multiple security elements: people, operations, technology, governance, and legal remedies [65]. The defence in depth is an essential principle in the choice of security needs against various threats. It aims to increase the effort required to succeed in an attack beyond sensitive data across government agencies.

Table 4.1: A Threat-Profile Model, adapted from [3]

Information Asset	Sensitive Data according to - Public Information Disclosure Act No. 14/2008 - National Intelligence Act No 17/2011
The Area of Concern	Sensitive Government Data and Services
Actor	Sophisticated and Well-Funded Adversaries (e.g. Foreign Intelligence Services) In this case, the five nations UKUSA Alliance 1) US — NSA (National Security Agency) 2) UK — GCHQ (Government Communications Headquarters) 3) Canada — CSEC (Communications Security Establishment Canada) 4) Australia — ASD (Australian Signals Directorate) 5) New Zealand — GCSB (Government Communications Security Bureau)
Means	Unauthorised Access Attacks (e.g Pervasive Surveillance Attacks): 1) ECHELON; 2) PRISM; 3) TEMPORA; 4) FAIRVIEW; 5) XKEYSCORE; and 6) STATEROOM
Motivate	Deliberate
Outcome	Disclosure
Security Requirement	Data Confidentiality
Probability	High
Consequences	1) It may disturb the protection of the right to intellectual property. 2) It may be hazardous to the defence and security of the state. 3) It could reveal the natural wealth of Indonesia. 4) It may be harmful to the national economic security. 5) It may be harmful to diplomatic relations. 6) It may reveal personal data and privacy
Impact Area	Government Security Privacy
Mitigation Controls	1) People; 2) Operations; 3) Technology; 4) Governance; and 5) Legal Remedies

4.2.2 Recruitment

The participant selection is an essential part of achieving both the validity and reliability of the study results. Since the motivation and experience of the participants directly affect the quality of findings, three relevant categories of participants, with valuable knowledge about government security needs, were chosen: government and military; industry; and government consultants. Three industry participants were from the major service providers

in Indonesia whose network infrastructure have been reported to be compromised according to the secret documents made public by Edward Snowdenr [11, 12]. The rest of the industry participants was from Indonesia's Internet Service Provider Association. Government consultants were security experts that have been working with the Government.

The participants of this study were chosen to achieve meaningful results and keep the failure rate as low as possible [159] according to the following the selection criteria: 1) work experience and background; 2) a self-critical attitude; 3) involvement in the policy-making process; and 4) a visible interest in the research topic.

The groups were formed based on expertise and background experience. This study invited 20 participants, consisting of eight participants from government and military officials, four participants from service providers and APJII, and eight participants as government consultants and experts. The majority of participants hold security certifications and have working experience more than ten years in government and industry sectors. The details of participants are not provided, to respect assurances of anonymity of all participants.

Further, there is no need to meet the participant number required for each group as expected by the Delphi criteria [128]. However, it is critical to ensure that the participants are qualified and knowledgeable to discuss the significant issues and propose the solution.

4.2.3 Procedure

For each round of Delphi, participants were asked to respond to the following questions:

Round 1: General. Participants were asked to express their opinions about the reasonable efforts to strengthen government security systems from breaches by protecting sensitive data of the country, in particular, how to mitigate unauthorised access to government networks, services and sensitive government data and assets in connection with the secret documents made public by Edward Snowden.

Round 2: Enrichment. By using the same question used, participants were asked to express further ideas about the available strategies based on the previous results. Participants were

asked to generalise the results/information and propose a list of government security needs.

Round 3: Integration. Participants were asked to consolidate all the results from each group of participants. Finally, participants were asked to propose a list of government security needs to a senior government official for review.

4.2.4 Data Collection and Analysis

The Delphi study took several months to complete, and consisted of three rounds of the Delphi study, as shown in Figure 4.1:

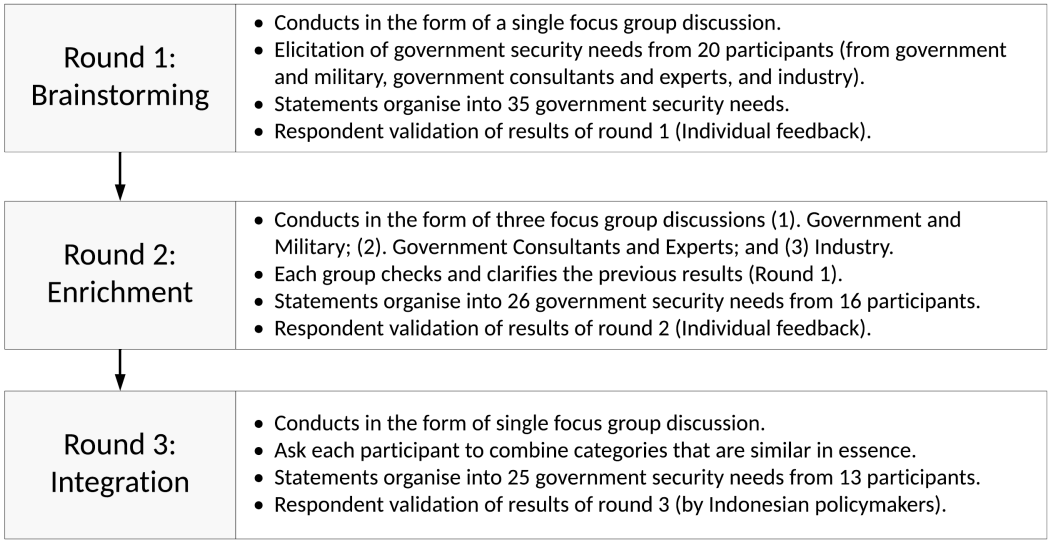


Figure 4.1: Phases of the adaptive Delphi study

This study adapted the features of a Delphi process to make separate group discussions for the second round to gather specific group responses, as each group was distinctive regarding participants' affiliations. Each group was required to identify specific and reasonable security needs. Participants described their opinions concerning government security needs. In the following process, each group was asked to make consolidated statements concerning the government's security needs. The security needs obtained from each group were summarised and combined into an initial set of categories of government security needs. In the latter process, this study conducted a consolidated meeting for validation between participants and the Indonesian policymakers.

Furthermore, this study took seven stages for data collection and analysis, as follows: 1) participant selection; 2) kick-off meeting; 3) first individual feedback; 4) three separate group discussions; 5) consolidated results and second individual feedback; 6) consolidated meeting for validation; and 7) government review and approval.

The first step, this study selected a moderator and formed four groups of participants with three to eight participants for each group [128]. In this step, the senior Indonesian policymakers were asked to advise on potential participants. Afterwards, this study selected the participants based on their confirmation.

The second step was the kick-off meeting where the moderator delivered a presentation and provided related documents to the participants. All participants were asked to create a list of security needs, and each participant expressed their opinions and comments on the list of security needs.

The third step, after the kick-off meeting, each participant was asked to review and revise the list of security needs based on the previous results. Each participant sent individual statements on such results by e-mail [115]. The individual feedback was incorporated into the results of the first round.

The fourth step was a series of distinctive group discussions, in which each group discussed the list of security needs derived from the previous steps. This second round results in a narrowing of the list of security needs through distinctive group discussions, pointing to some clarification and asking each participant to sharpen a priority of security needs regarding the protection of sensitive government data from unauthorised access.

In the fifth step, the moderator summarised the results from group discussions and asked each participant to review and revise the security needs. All individual feedback was conducted through email, and only the moderator knew who proposed and generated such security needs.

The final step was a consolidated meeting of the participants of this study with senior Indonesian policymakers to review and validate the initial set of categories of government security needs. The result of the third round was a list of 25 categories of government security needs.

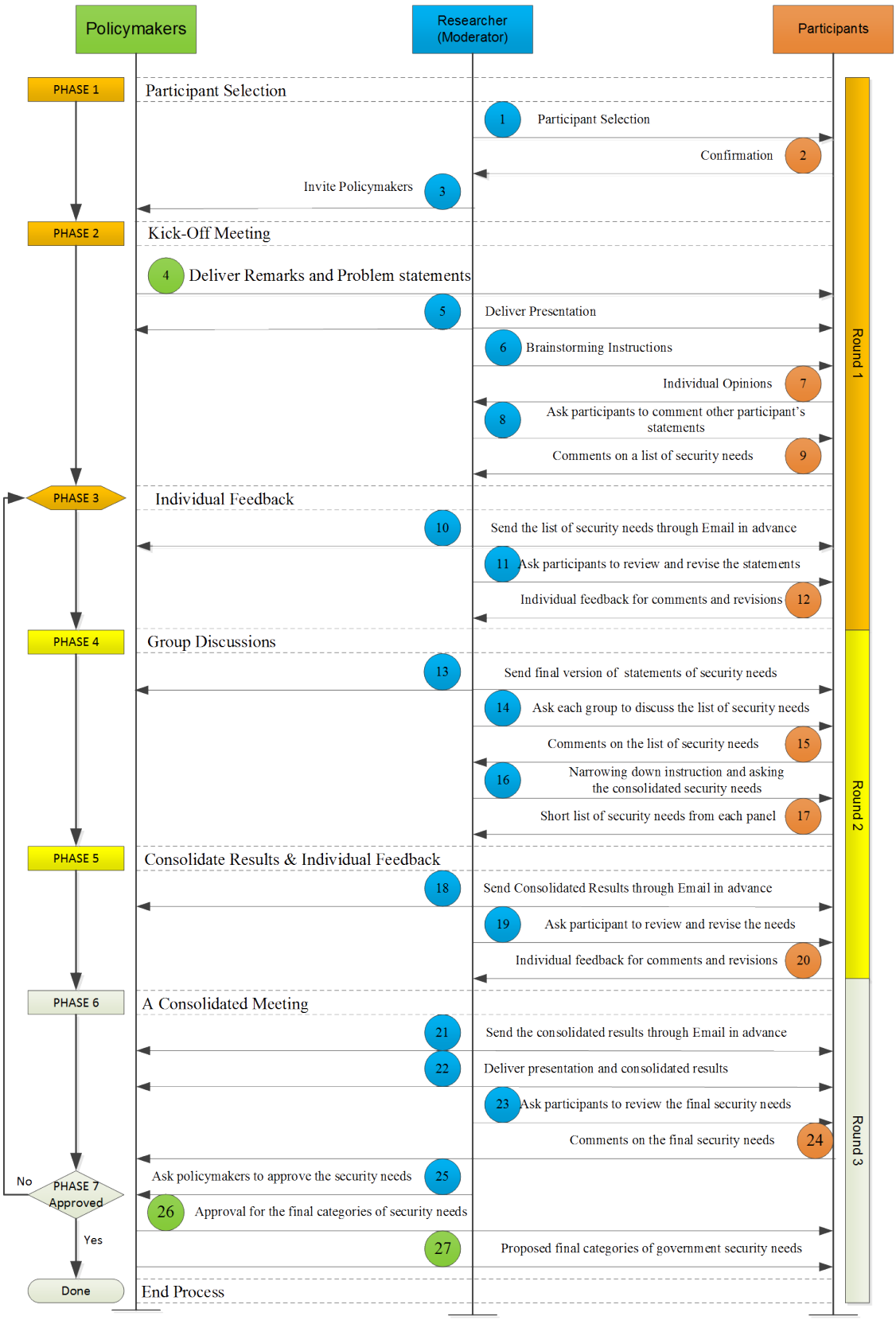


Figure 4.2: Adaptive Wideband Delphi Framework

4.3 Findings

This section presents the findings of the adaptive wideband Delphi study. Based on the Delphi framework as shown in figure 4.2, this chapter identifies 25 categories of the Indonesian Government security needs to protect sensitive government data against unauthorised access. The results showed that participants stated these security needs were based on their perception of the state's national interests in a three-round Delphi study. As seen in figure 4.3, in the first round, 35 categories of government security needs were distributed into a five-defence in-depth element. In the second round, 26 categories of government security needs were identified in five elements. In the third round, 25 categories of government security needs were proposed and mapped into the five defences in depth elements.

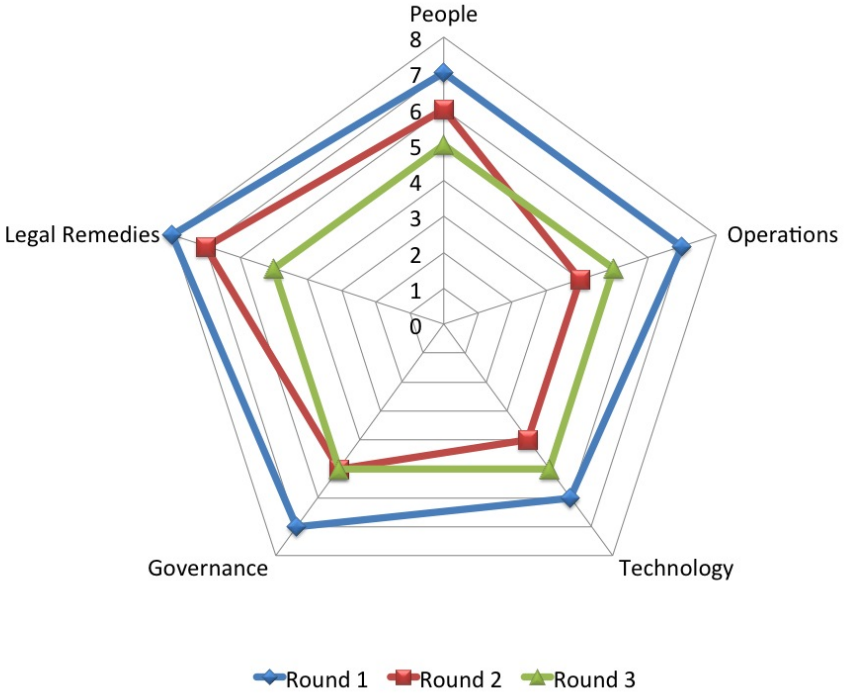


Figure 4.3: Distributed Statements for Government Security needs

It noted that some participants failing to mention a particular security need does not mean that it is irrelevant to such participants. For example, the top priority of security needs from the Government group was 'security awareness'. Other groups also listed such security need. However, not all groups selected the same categories of security needs. This view

supports the methodology of gathering opinions and statements from multiple stakeholders, as it enables a comprehensive coverage of all aspects of the topic discussed that is being discussed during the Delphi rounds.

It was difficult to propose statements concerning government security needs across multiple stakeholder settings. However, the method used in this study offers flexibility that each participant was encouraged to identify categories of government security needs based on their expertise and experiences to increase the originality of their opinions. The major categories of selected security needs were almost the same for each round because the levels of consistency on the security needs selected were moderately strong within the three-round Delphi study.

Based on the findings of this study, it shows in Table 4.7 that there are some novel concepts of the Indonesian Government security needs, while other security needs are correlated with some security controls listed in ISO/IEC 27002 [160], NIST SP 800-53 [1] and 20 Critical Security Controls [158]. The 25 categories of government security needs are a combination statement from the Delphi's participants and framed by the five defences in-depth security elements of people, operations, technology, governance, and legal remedies. In this chapter, each security need is written as an obligation on how the Government preserve the confidentiality of sensitive data. Thus, the terminology for this study follows the general format '*The Government of Indonesia should...*' [161].

4.3.1 People

For people factor, participants were asked to indicate the government's security needs that represented appropriate controls for human factors in security. Participants discussed the need for developing a security culture and mindset. However, the participants focused on management commitment to information security and personnel security including security awareness. The findings of this study consolidate the integration of security needs-related people into five main categories, namely: 1) awareness, training and education; 2) information security commitment; 3) non-disclosure agreement; 4) security clearance proving; and 5) local experts requirement, as shown in Table 4.2.

Table 4.2: Risk and Need of People Element

Risk	Need	Description	Reasonable Effort
Awareness and Skills	Awareness, Training and Education	The Government should provide evidence that all employees receive appropriate security awareness, training and education for protecting sensitive data according to the laws and regulation	This need helps ensure that an effort has been made to develop security awareness policy, security culture and mindset within the organisation
Leadership	Information Security Commitment	The Government should provide evidence that sensitive information owners actively support the implementation of information security policy within the organisation	This need helps ensure that top management demonstrates their commitment to establishing an information security framework.
Rules and Compliance	Non-Disclosure Agreement	The Government should provide evidence that non-disclosure agreement for protecting sensitive data and assets exists two or more contracting parties and is regularly reviewed.	This need helps ensure that the organisation preserves authorised restrictions on information access and disclosure, including means for protecting sensitive information.
Insider Threat	Security Clearance Proving	The Government should provide evidence that a set of formal screening process applies to all employees, supplier, contractors and third-party relationships	This need helps ensure that security clearance proving should be implemented for all entities, including personnel security mechanism before employment, during employment and termination of employment.
Human Resources	Local Experts Requirement	The Government should provide evidence that critical infrastructure owners shall employ local experts in certain areas.	This need helps ensure that reasonable effort has been made to manage serious impacts on state defence and security.

Based on the Delphi results, security awareness is a significant concern raised by the participants. In particular, security awareness for those people who have access to sensitive government data and assets. The statements from the participants suggest that the government should enhance security awareness policy, including developing security culture, behaviours and security mindset.

It is clear that human elements are significant vectors of security risks that can be delivered by individual employees, suppliers, service providers, contractors and external collaborators. In this case, various security risks-related to human elements, such as the absence of awareness and skills, strong leadership and rules and compliance can be vulnerable to unauthorised access to sensitive government data. Such risks can increase because of the insider threat and the use of foreign workers. The findings of this study summarise the associated risk in each government security need in Table 4.2.

Furthermore, it is evident that some security needs are associated with other security controls listed in ISO/IEC 27002 [66], NIST SP 800-53 [1] and 20 Critical Security Controls [158]. Most of the security controls listed in such catalogues cover security needs-related human elements except local experts requirements. A summary of related controls regarding the 25 categories of government security needs is described in Table 4.7.

4.3.2 Operations

For operational elements, participants were asked to discuss operational measures to improve security mechanisms for the Government's information systems. The majority preference was to establish a security incident response team and security continuous monitoring. Other security needs focus on all the activities required to sustain organisations' security posture or compliance with standards, policies and regulations on a day-to-day basis. The findings of the Delphi study consolidate the integration of security needs-related operational elements into five main categories, namely: 1) trustworthy system certification; 2) authorised software inventory; 3) authorised hardware inventory; 4) incident response management; and 5) security continuous monitoring, as shown in Table 4.3.

Based on the statements collected, it is clear that the government wants to build a trustworthy ecosystem through certification and attestation schemes based on standards. However, the existence of known or unknown vulnerabilities, including backdoors and zero-day exploits within information systems (e.g. hardware, software or source code) can be exploited by a range of adversaries in an attempt to obtain sensitive government data. The comments from the participants suggest that the government should make reasonable efforts to assure that hardware devices and software applications should be certified and attested to the formal security evaluation.

In this case, the most important risk factor is the lack of trusted electronic systems used for the government's information systems. Consequently, if combined with other security risks, such as zero-day attacks and discontinuity controls and monitoring, it can lead to vulnerabilities because adversaries can get access to sensitive government data and services. The findings summarise the associated risk in each government security need in Table 4.3.

Table 4.3: Risk and Need of Operations Element

Risk	Need	Description	Reasonable Effort
Trusted Electronic System	Trustworthy System Certification	The Government should provide evidence that the certification and attestation process exists in any critical government information systems.	This need helps ensure that all critical government information systems should be certified and attested by formal security evaluation to increase reasonable levels of trustworthiness.
Software Vulnerabilities	Authorised Software Inventory	The Government should provide evidence that adequate controls of authorised software inventory exist to minimise security risk.	This need helps ensure that a reasonable effort has been made to assure that software platforms do not contain any malicious code and known vulnerabilities
Hardware Vulnerabilities	Authorised Hardware Inventory	The Government should provide evidence that adequate controls of authorised hardware inventory exist to minimise security risk.	This need helps ensure that all devices that are handling sensitive data are subjected to the formal security evaluation
Incident Response	Incident Response Management	The Government should provide evidence that the organisation can detect and respond attacks on any critical government information systems	This need helps ensure that any incidents are appropriately investigated and recovered rapidly.
Control and Monitoring	Security Continuous Monitoring	The Government should provide adequate procedures for continuous security monitoring of unauthorised access or disclosure to sensitive information	This need helps ensure that sensitive information is regularly monitored to identify any security events.

Furthermore, the overall findings highlight that the existing security controls cover such selected security needs, except one security need regarding *trustworthy systems certification*. Details of related controls are listed in Table 4.7.

4.3.3 Technology

From the technology aspect, participants consolidated the integration of security needs related technical controls into five main categories to protect government information systems. These categories are: 1) system and communications protection; 2) national cryptographic standard; 3) local applications platform; 4) national infrastructures platform; and 5) international traffic control, as shown in Table 4.4.

Participants pointed out that it was essential to strengthen national security capabilities to reduce risks related to pervasive surveillance attacks by using appropriate technologies. For instance, participants stated that using local cryptographic tools, secured networks

and devices provided by the Indonesian National Crypto Agency could protect sensitive government data. Moreover, participants were clear about the government security needs for the establishment of national security capabilities, primarily to protect the confidentiality, integrity and availability of sensitive government data.

Table 4.4: Risk and Need of Technology Element

Risk	Need	Description	Reasonable Effort
Networks Infrastructure	System and Communications Protection	The Government should provide evidence that access to government networks is appropriately controlled and reasonably secured.	This need helps ensure that a reasonable effort has been made to mitigate network attacks.
Information Architecture	National Cryptographic Standards	The Government should demonstrate compliance with national cryptographic standards to protect the confidentiality and integrity of sensitive information.	This need helps ensure that reasonable effort has been made to protect sensitive information according to applicable laws and regulation across government agencies and public organisations.
Platform	Local Applications Platform	The Government should enforce sensitive information owners to use in-house applications platforms to minimise risks of pervasive surveillance attacks of data gathered by global platforms.	This need helps ensure that government agencies and public organisations utilise local applications platform for ensuring the confidentiality of sensitive data.
Backbone Dependencies	National Infrastructures Platform	The Government should enforce sensitive information owners to use the national infrastructure platform to minimise risks of pervasive surveillance attacks of data traffic transited through international gateways.	This need helps ensure that the national infrastructure communications should be utilised in accessing and delivering sensitive information within government information systems.
Information Flows	International Traffic Controls	The Government should provide evidence that international traffic controls requirements exist, and sensitive information flow is controlled regularly.	This need helps ensure that the government has a procedure for protecting sensitive information, which is intended to deliver to other entities outside the government information systems.

In this case, Indonesia's domestic Internet connectivity is highly dependent on international backbones. However, the Government have developed 'a Palapa Ring Project', a Fibre Optic Backbone Infrastructure, which aims to expand the national gateway for Internet connectivity within a national border. This initiative is relevant to the idea of safeguarding and protecting sensitive government data against pervasive surveillance attacks. Furthermore, the existence of zero-day exploits and the absence of information flow control increases vulnerabilities to unauthorised access and data exfiltration. Additionally, some potential

threats to the confidentiality of sensitive government data have been growing due to the level of control over the Internet by the NSA and its international partners. The findings of this study outline the associated risk in each security need in Table 4.4

In this case, existing security controls only cover two security needs regarding the system and communications protection and cryptographic control. Other three security needs seem to be novel for the Government to mitigate unauthorised access to sensitive government data. Related controls are reported in Table 4.7.

4.3.4 Governance

Participants were asked to discuss governance frameworks to mitigate unauthorised access to sensitive government data against pervasive surveillance attacks. The findings of this study indicate five categories of government security needs, namely: 1) independent review agency; 2) risk management process; 3) information security baseline; 4) potential threat impact; and 5) domestic hosting and domains, as shown in Table 4.5.

Table 4.5: Risk and Need of Governance Element

Risk	Need	Description	Reasonable Effort
Control Deficiencies	Independent Review Agency	The Government should provide evidence that any critical government information systems that directly affect national security are subjected to review by an independent agency who is responsible for national security.	This need helps ensure that security mechanisms, including security risk assessments, exist to protect sensitive data and assets.
Damage and Lost	Risk Management Process	The Government should enforce sensitive information owners to apply risk management systems for any damage which may arise.	This need helps ensure that risk management approaches should exist and are regularly managed.
Compliance and Control	Information Security Baseline	The Government should have a written policy for implementation information security baseline within government information systems	This need helps ensure that is an implementation of information security management systems should exist as minimum requirements.
Escalation Process	Potential Threat Impact	The Government should provide evidence that potential threat impact has been established for efficiently managing, identifying, mitigating and escalating threats	This need helps ensure that vulnerabilities and threats to sensitive government data and assets regarding critical government information systems are identified and documented.
Trust	Domestic Hosting and Domains	The Government should enforce sensitive information owners to use Domestic Hosting and Domains, such as the use of ccTLD	This need helps ensure that a reasonable effort has been made to protect the whole people and the entire homeland of Indonesia.

Participants in this study pointed out that the development of national hosting and domains, such as a national email service and national hosting would allow Indonesian

citizens to keep their data within areas of national jurisdiction. The comments from the participants suggest that the Government should take reasonable efforts to keep the citizen's data out of the reach of foreign companies, such as global cloud service providers (e.g. Microsoft Azure). These efforts take a position beyond the domination of U.S. global infrastructure networks and services. One impressive result is that the participants stated a preference for the use of Indonesia's national top-level domain - (.id).

Further, several risk scenarios need to be understood to provide enough information about the best approach to mitigate pervasive surveillance attacks. The majority of participants stated that a significant risk factor was a lack of trust within Indonesian organisations, such as not using local domain names. If combined with other risks (e.g. the absence of compliance to security baseline and clarity around escalation procedures), these risks can lead to vulnerabilities of which could be exploited by internal or external attackers.

The results of this study summarise the associated risk in each security need in Table 4.5. Moreover, this study identifies some security controls from ISO 27002 and NIST SP800-53 fit such security needs, except the Critical Security Controls. One unique security need was the utilisation of national domain names. Thus, there is no related controls exist regarding such security need. A summary of appropriate controls is summarised in Table 4.7.

4.3.5 Legal Remedies

In this section, the Delphi's participants were asked to discuss legal remedies to mitigate pervasive surveillance attacks. The findings of this study identify five categories related to legal needs. In essence, the majority preference was to include contractual information security agreements, data protection regulation and data localisation policy. Overall, this study consolidates the integration of the government's security needs-related legal remedies into five categories, namely: 1) information security agreement; 2) data protection regulation; 3) data centre localisation; 4) lawful interception capability; and 5) ethics code and conduct, as shown in Table 4.6.

The statements from the participants suggest that the Government should establish data protection regulation to encourage good information security practice within the govern-

Table 4.6: Risk and Need of Legal Remedies

Risk	Need	Description	Reasonable Effort
Agreement	Information Security Agreement	The Government should provide evidence that information security agreement between public organisations and external parties are in place to minimise risks of pervasive surveillance attacks.	This need helps ensure that availability of information security agreement should exist for any critical national infrastructure sectors, such as government agencies and public organisation.
Data Protection	Data Protection Regulation	The Government should provide evidence that a set of data protection requirements are established to regulate the scenarios from which data can be collected and stored by public sector organisations, and external entities	This need helps ensure that an effective data protection regime should be in place to protect the security and privacy of sensitive government data and assets.
Cross-Border Information	Data Centre Localisation	The Government should provide evidence that a set of security requirements are established to place a data centre and disaster recovery centre in the country.	This need helps ensure that data sovereignty can be attained for law enforcement and protecting citizen's data.
Lawful Interception	Lawful Interception Capability	The Government should provide evidence that lawful intercept capability laws are in place to enable necessary and proportionate communications surveillance by intelligence and law enforcement agencies.	This need helps ensure that an intelligence collecting process is regulated including mechanisms for lawfully obtaining raw data.
International Cooperation	Ethics Code and Conduct	The Government should provide evidence that a set of protocol and code of ethics are acknowledged when establishing bilateral cooperation with other countries.	This need helps ensure that an effort has been made to protect sensitive information that cannot be disclosed under the laws and regulation.

ment agencies and public or private sector organisations. Legal remedies related to data localisation requirement is paramount of importance in protecting and safeguarding national interests, primarily for law enforcement and protecting citizen's data against force majeure (e.g. earthquakes, floods and wars).

It seems clear that any governments should build their security capabilities to protect national interests against foreign intelligence services as well as to conduct surveillance activities in support of its national interests. However, it is essential to bear in mind that such intelligence agencies also have an essential role in safeguarding and protecting the state's national interests such as protecting national security, ensuring the economic well being of the state, and preventing serious crime.

The most important aspect is to establish information security agreements, including the code of ethics and conduct between government agencies and external entities (e.g. foreign service providers). This view is related to Article 12, paragraph 1 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, all service providers who operate in Indonesia have obligations to have agreements on service level and security when providing such information technology services [13].

The findings of this study summarise the associated risk in each security need in Table 4.6. Furthermore, only security controls listed in ISO/IEC 27002 and NIST SP800-53 cover such security needs, and none of the Critical Security controls fits the security needs, except data protection control. A summary of related controls is listed in Table 4.7.

Overall, the emphasis placed on the security needs were prominent to extend that participants referred to them as 'basic' needs for a government security framework. To this end, participants were asked to rate needs statements on a sliding scale of 'importance'. In doing so, the participants were allowed to express the same security needs. The results were not used for ranking purposes but did help to classify some government security needs according to their priority. Using this scale, four categories of government security needs stood out as receiving a high rating from all groups, namely: 1) security awareness; 2) strong leadership; 3) data protection regulation; and 4) information security agreements.

Given the importance attributed to such basic government security needs, there is indeed justification for further research. The Government should provide evidence that such basic security needs can be implemented efficiently against unauthorised access to sensitive government data and assets, especially posed by a range of threats, including insider threats and advanced, sophisticated threats (e.g. foreign intelligence services).

4.4 Discussion

This section compares the findings of this study with related work, and elaborates on the implications of the findings for the Government and makes concrete recommendations for how the findings can most fruitfully direct their efforts to mitigate unauthorised access to sensitive government data.

4.4.1 Reflection on related works

The related work refers to existing security controls sets from ISO/IEC 27002, NIST SP800-53 and 20 Critical Security Controls. Overall, the Delphi study identifies the 25 categories of government security needs for preserving the confidentiality of sensitive government against sophisticated and well-funded adversaries. Some government security needs are relevance

Table 4.7: Mapping needs for other security controls sets

ID	Requirement	National Interests				Mapping to		
		NI1	NI2	NI3	NI4	ISO 27001:2013	NIST SP 800-53 Rev.4	CCS CSC
1	Awareness, Training and Education	X		X		A.6.1.1 A.7.2.2	AT-1, AT-2, AT-3 PS-7, SA-9, PM-13	CCS CSC 9
2	Information Security Commitment	X		X		A.5.1.1, A.6.1.1 A.7.2.1	PM-1, PM-2, PM-3	None
3	Non-Disclosure Agreement	X		X		A.13.2.4	PS-6	None
4	Proof of Security Clearance	X		X		A.7.1.1	PS-3, SA-21	None
5	Local Experts Requirement	X		X		None	None	None
6	Trustworthy Systems Certification	X			X	A.14.2.8, A.18.2.1, A.18.2.2, A.18.2.3.	SA-13, CA-2, CM-4	None
7	Registration of Authorised Software	X			X	A.8.1.1, A.8.1.2, A.14.1.1, A.14.1.2, A.14.2.6	CM-8, CM-10, SA-3, PM-5	CCS CSC 2
8	Registration of Authorised Hardware	X			X	A.8.1.1, A.8.1.2, A.14.1.1, A.14.2.9	CM-8, IA-3, SA-4 SI-4, PM-5	CCS CSC 1
9	Incident Response Management	X			X	A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6	IR-4, IR-6, IR-8, AU-6	CCS CSC 18
10	Security Continuous Monitoring	X			X	A.12.2.1, A.12.4.1, A.12.6.1, A.14.2.7, A.15.2.1	SI-3, AU-6, AU-13 RA-3, RA-5, SA-9, SA-11,SA-12,CA-8	CCS CSC 4, 5 CCS CSC 14 CCS CSC 16
11	System and Communications Protection	X	X			A.8.2.3, A.13.1.1 A.13.2.1, A.13.2.3 A.14.1.2, A.14.1.3	PE-20, SC-8, SC-7, SC-11, SC-28, CA-3, SC-13	CCS CSC 17
12	National Cryptographic Standards	X	X			A.10.1.1, A.10.1.2 A.14.1.2, A.14.1.3 A.18.1.5	SC-12, SC-13, SC-17	CCS CSC 17
13	Local Applications Platform	X	X			None	SC-27	None
14	National Infrastructure Platform	X	X			None	None	None
15	Control of International Traffic	X	X			None	None	None
16	Agency of Independent Review	X	X		X	A.14.2.8, A.18.2.1 A.18.2.2, A.18.2.3	CA-1, CA-2, CA-7 SA-11	None
17	Risk Management Process	X	X		X	A.12.6.1	PM-9, PM-8, SA-14 RA-3	CCS CSC 4
18	Information Security Baseline	X	X		X	A.14.1.1, A.14.2.5	PL-2, PL-7, PL-8, SA-8	CCS CSC 3, CCS CSC 10, 11
19	Impact of Potential Threat	X	X		X	A.11.1.4, A.12.6.1, A.17.1.1, A.17.2.1	CP-2, PM-9, RA-3	CCS CSC 8
20	Domestic Hosting Domains	X	X		X	None	None	None
21	Information Security Agreement	X	X		X	A.13.2.2, A.15.1.2	SA-4, SA-12, PS-6, SA-9	None
22	Regulation of Data Protection	X	X		X	A.8.2.1, A.18.1.4	SI-12, RA-2	CCS CSC 17
23	Data Centre Localisation	X	X		X	None	None	None
24	Lawful Interception Capability	X	X		X	None	None	None
25	Code of Ethics and Conduct	X	X		X	A.18.1.1	None	None

to existing security control sets, except local experts requirements, trustworthy system certifications, national infrastructure platforms, international traffic controls, domestic hosting and domains, data localisation requirements and information security agreements.

Comparing the findings of this study with another related work, Bauman et al. [55] also outlines some government security needs from the German and Brazilian governments against pervasive surveillance attacks. Those security needs are the creation of local data clouds, national routing, development of surveillance capabilities, investment in security professionals and intelligence experts. Both governments have also attempted to develop domestic content, such as a national social media and email as well as international Internet connectivity beyond the scope of the US Internet infrastructure. Based on the findings and literature, it is clear that the secret documents made public by Edward Snowden have built a distrust of other countries outside the Five Eyes countries, which is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States.

Further, all security needs are in line with national interests. In this case, the preamble of the 1945 constitution of the Republic of Indonesia states four national interests (NI), namely: 1) to protect the whole people of Indonesia and the entire homeland of Indonesia (NI1); 2) to advance general prosperity (NI2); 3) to develop the nation's intellectual life (NI3); and 4) to contribute to the implementation of world peace (NI4). A mapping of security needs to three existing security guidelines is summarised in Table 4.7.

Therefore, it is expected that the implementation of the government's security needs will help ensure to mitigate unauthorised access to sensitive government data and to increase public trust. The statements from the participants suggest that concrete steps are needed to meet and implement such government security needs. It is inevitable that the implementation of such security needs will take time and may differ in details across government agencies.

4.4.2 Main Outcome

From the perspective of the Indonesian Government, this chapter considers the following takeaway to be the most important ones from the findings:

- The Government commonly makes decisions about the policy of procuring external information system services offered by third-party service providers, such as cloud-based services. However, the limited adoption of certifying levels of security for services can be an indicator of a lack of security assurance from service providers.

- The Government faces technical challenges, including the absence of the government's security considerations for public procurement and limited data confidentiality requirements for protecting sensitive government data when the government's information systems operated by service providers on behalf of the Government.

- Certification schemes (e.g. ISO/IEC 27001) play an essential role in the implementation of public procurement policy for government agencies. In procuring high assurance systems, the Government sometimes introduces additional security controls into the requirements.

- A critical reason for the failure of some security controls listed in ISO/IEC 27002, NIST SP800-53 and 20 Critical Security Controls is their incompatible with the government security needs. Some security needs are not linked to the existing security controls because the security needs seem to be novel for the Government to mitigate unauthorised access to sensitive government data.

4.4.3 Recommendations

The findings raised by this study indicate several recommendations on which the Government can focus its efforts, as follows:

- **Understand Human Security**. Human elements are a current weakness in Indonesia. The development of security awareness, security mindset and behaviour are the biggest challenges. It means the Government should better prepare society for information security. This condition is because people may also be the greatest strength when organisations can develop an internal culture of security. Therefore, it is important to promote ethical behaviour and employee vigilance.

- **Establish Strong Leadership**. A lack of strong leadership including governance and coordination exists due to ambiguity concerning shared responsibilities. The Government should establish and maintain an information security governance framework to overcome such problems.

- **Develop Appropriate Level of Security Protection**. Security mechanisms are needed to protect sensitive government data and assets including critical information infrastructures that may impact state sovereignty, and people's safety, prosperity, and well-being. The location and potential path of sensitive government data and assets should be understood to implement effective technical requirements and responses. Therefore, it allows various technical controls to be implemented to protect sensitive government data and assets in layers.

- **Develop Data Protection Regulation and Protocols**. The challenge of securing sensitive government data remains a hard problem, especially given the absence of data protection laws and regulations which provide organisations with an assurance that sensitive government data and assets will be protected from unauthorised access. Even though the Government has passed some laws addressing information security (the Telecommunication Law Number 36 of 1999, the Electronic Information and Transactions Law Number 11 of 2008, and the Government Regulation on Electronic System and Transaction Operation Number 82 of 2012), Indonesia is weak in data protection regulation. Therefore, the Government should have complete control over sensitive government data and assets when using external information system services.

- **Develop Government Security Classifications**. Classifying government data is of fundamental importance in the government context and should be formulated explicitly by adequate security controls designed to meet legal and technical requirements. For example, suppliers or service providers that work with the Government have respect for the confidentiality and integrity of any sensitive government data. Therefore, the Government should classify government data into several categories, and each has an adequate level of security protection against applicable threats.

- **Strengthen Trust-Enhancing Instruments**. In the government scenario, when protecting sensitive government data, the focus is often placed on what sensitive data cannot be disclosed to third parties through a non-disclosure agreement (NDA) as one example of government security needs described in the current study. However, such an agreement is not well-suited to the service scenario, especially when using external information system services. The business relationships with service providers are formally established through contracts or service level agreements (SLAs). This view is related to the findings of this research of which information security agreements are essential between customers and service providers. Notably, under Article 12, paragraph 1 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, all service providers that provide information technology services in Indonesia have obligations to have agreements on service level and security [13]. The Government should provide evidence that information security agreements between government agencies and service providers are essential to develop trust relationship and guarantee a level of assurance and satisfaction that can meet the Government's security needs against unauthorised access to sensitive government data.

4.5 Chapter Summary

This chapter has described a combination of the Wideband Delphi method and traditional Delphi study that developed to understand the Indonesian Government's security needs to mitigate unauthorised access to sensitive government data, especially posed by global adversaries like foreign intelligence services. The variant includes three rounds of the Delphi technique to achieve consolidation among participants, with review and approval from a senior Indonesian official. By testing this method with the Indonesian Government, this chapter has found that further rounds would have yielded diminishing returns, particularly regarding participating participants in further meetings.

Overall, this chapter has investigated the Indonesian Government's security needs to mitigate unauthorised access to sensitive government data and assets, especially in response

to pervasive surveillance attacks posed by sophisticated and well-funded adversaries. This study was designed to elicit the statements of government security needs across multiple stakeholders settings (government and military, government consultants and experts and industry) to mitigate such threats using an adaptive Delphi method. This chapter has identified 25 categories of government security needs which are framed by the five primary elements: people; operations; technology; governance; and legal remedies. The findings of this study may not apply to other governments, but such methods may be applied to other settings (e.g. other governments).

Further, the statements from participants suggest that the Government should more focus on its efforts into security awareness, strong leadership, data protection regulation and information security agreements. Such priorities will serve as a base for future studies. A study investigating government security needs in contracts or service level agreements (SLAs) would be interesting. Such a recommendation is relevance to the findings that information security agreements should be established between government agencies and external entities including suppliers, service providers and contractors. Therefore, future research should concentrate on the investigation of the perception of government SLA data confidentiality requirements from the Government experts.

5

Government Service Level Agreement Data Confidentiality Requirements

> *Security requirements for external service providers including the security controls for external information systems are expressed in contracts or other formal agreements.*
>
> NIST SP 800-53 Rev.4,

Chapter 5 draws on refereed articles described in the following publications:

- Y. Nugraha and A. Martin. Investigating SLA Confidentiality Requirements: A Holistic Perspective from the Government Agencies. In Proceedings of 11th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2017), pp. 154-160, IARIA, 2017 [162].
- Y. Nugraha and A. Martin. Understanding Government Service Level Agreement Confidentiality Requirements: An Indonesian Government Case Study. This manuscript is in the process of submission to a journal publication.

Contents

5.1 Introduction

Government agencies are increasingly relying on external service providers to help support government tasks and functions using available computing, communications and storage solutions in delivering public services. Consequently, many service providers routinely process, store, and transmit sensitive government data in their information systems to support the delivery of services to government agencies (e.g. processing healthcare data, providing financial services and providing cloud-baded services). The level of trust with service providers is usually established through non-disclosure agreements (NDAs), certification schemes and SLAs.

Further, as the previous chapter indicates, it is necessary to have NDAs, certifications or information security agreements as reasonable efforts to protect sensitive government data from unauthorised access. However, both NDAs and certification schemes are not well-suited to the service scenario while existing SLA definition only pays attention to the system availability and performance aspects without expressing data confidentiality and integrity in SLA contexts. Although the concept of security-related SLAs has been studied since 1999 [31–38], there appears to be a gap of understanding government SLA data confidentiality requirements.

Several governments have introduced a set of security requirements in the context of government scenarios for procuring external information systems services provided by external service providers [47, 59, 60, 62]. However, the formulation of SLA data confidentiality requirements has not been studied by academic researchers. This gap indicates a need to understand the perception of the government SLA data confidentiality requirements when using such external services from external service providers.

Therefore, this chapter seeks to fill the gap by understanding the government's perspective about SLA data confidentiality requirements, which are targeted at participants who are employed by or have experience working with government agencies using Indonesia as a case study. It is necessary to perceive what types of government assets to protect and what categories of risks to mitigate to increase the consideration of data confidentiality requirements in SLA definition. To this end, this study develops and conducts a grounded

adaptive Delphi method (GADM) with 35 government employees and government consultants, with group discussions and interviews to gauge an understanding of the SLA data confidentiality requirements for the context of the Indonesian Government. The data collection and analysis were performed in three phases: 1) brainstorming sessions using a series of group discussions; 2) enrichment sessions using individual interview sessions; and 3) an integration phase through a grounded theory analysis of the Delphi study data to categorise the extracted statements [106–108].

This chapter uncovers three increasing considerations of the Government's data confidentiality requirements when defining SLAs. The first consideration introduces 21 concepts within three main categories of the target of protection, namely: 1) human asset; 2) information asset; and 3) physical asset. The second consideration presents 17 concepts within five main categories of risk perception, which are: 1) collaborator; 2) exfiltration; 3) observation; 4) insertion; and 5) manipulation. The third consideration introduces 22 concepts within five main categories of government SLA confidentiality requirements, namely: 1) access management; 2) data management; 3) identity management; 4) malicious management; and 5) compliance management. The findings can be used to guide the development of foundations for a TDSLA capability framework.

The remainder of this chapter is structured as follows. Section 5.2 describes how to investigate the perception of government SLA data confidentiality requirements, including participant selection and data collection and analysis of findings. Section 5.3 presents the findings of the study. In Section 5.4, this chapter discusses how the findings compare with related work, and elaborates on the implications of the findings for concrete recommendations. Section 5.5 summarises the chapter.

5.2 Method

5.2.1 Aim

This chapter investigates an understanding of government SLA data confidentiality requirements using 35 participants (government employees and government consultants) based

in Indonesia using a grounded adaptive Delphi study [13]. A significant impetus for this research emerged from Article 12 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions, Number 82 of 2012. The Government Regulation states that electronic system operators including service providers have obligations to ensure agreements on minimum service level and information security when providing such external service provisions to customers, including government agencies.

Four-phase of data collection and analysis was conducted to conclude the objective of this study from different perspectives and experiences. These phases are namely: 1) recruitment; 2) a brainstorming phase using several group discussions; 3) an enrichment phase using individual interviews; and 4) an integration phase through a grounded theory analysis of the Delphi study data to categorise the statements from participants [106–108].

5.2.2 Recruitment

This study began with a research proposal submitted to the Government Ministry which administers information assurance and security in Indonesia. After receiving a confirmation and approval from an official, this study recruited participants for the Delphi study via existing connections to government employees including government consultants, usually via verbal or email communications with the participants. All participants received an official invitation letter signed by a senior official, including participant information sheets and consent forms. The study selected participants based on participants' technical expertise and their involvement in the policy-making process to achieve meaningful results and keep the failure rate as low as possible [14]. Overall, this study engaged with 35 of 45 invited participants. Most group discussions and individual interviews were conducted in-person, although some were conducted via Skype.

In this study, participants were civil servants and government consultants working with the Indonesian government. This focus aimed to explore the problem of preserving the confidentiality of sensitive data across government agencies. Further, the participants of this study had diverse work experience and technical backgrounds, such as cyber defence experts, malware experts, cryptography experts, pen-testers, and information security management

experts. Additionally, the majority of participants hold security certifications, and 12 participants hold a PhD degree in information technology-related topics. Each participant identified as P1 to P35 to maintain anonymity and confidentiality. A summary of the participants is presented in Table 5.1.

5.2.3 Procedure

Each group discussion and interview within the Delphi study took between 60 - 120 minutes. For each round of Delphi, participants were asked to discuss how to incorporate the Government's data confidentiality requirements specified into SLA contexts. For this purpose, participants were asked to respond to the following questions:

- What information assets are of most value to government agencies;
- Why are such information assets critical to government agencies;
- Is this information asset electronic or physical, or both;
- What information systems are used to process, store or transmit such information asset;
- Are there suppliers, service providers or contractors that process, store or transmit such information asset;
- What are areas of concern that could affect the confidentiality of information assets; and
- What confidentiality requirements are needed for a given area of concern.

Finally, participants had an opportunity to share any additional thoughts and opinions. Moreover, participants were allowed to elaborate on their experiences beyond the questions above, which were used for guidance only to gain more information from participants. By doing so, the responses to the questions were in-depth and meaningful and allowed for new themes or patterns to emerge, based on real experience.

Table 5.1: Participants' Information and Experience

Participant					
Identifier	*Gender*	*Role*	*Years' Experience*	*Education*	*Category*
P1	Male	Director General	26–30	PhD	Civil Servant
P2	Male	Vice Chairman	21-25	PhD	Civil Servant
P3	Female	Crypto expert	16-20	PhD	Consultant
P4	Male	Defence expert	21-25	PhD	Consultant
P5	Male	Security expert	16-20	PhD	Consultant
P6	Male	Security expert	21-25	MSc	Consultant
P7	Male	IT expert	21-25	MSc	Consultant
P8	Male	Security expert	21-25	PhD	Civil Servant
P9	Male	Defence expert	21-25	MSc	Civil Servant
P10	Male	IT expert	16-20	MSc	Civil Servant
P11	Male	Director General	31-35	PhD	Civil Servant
P12	Male	Vice Chairman	21-25	(PhD)	Consultant
P13	Male	Malware expert	21-25	(PhD)	Consultant
P14	Male	Pentester	16-20	MSc	Consultant
P15	Male	Vice Chairman	21-25	(PhD)	Consultant
P16	Male	Security expert	21-25	MSc	Consultant
P17	Male	Security expert	16-20	MSc	Civil Servant
P18	Male	Security expert	16-20	MSc	Consultant
P19	Male	Crypto expert	16-20	PhD	Civil Servant
P20	Male	Security expert	21-25	MSc	Consultant
P21	Male	Director	26-30	MSc	Civil Servant
P22	Male	Deputy Director	26-30	MSc	Civil Servant
P23	Male	Deputy Director	26-30	MSc	Civil Servant
P24	Male	Deputy Director	11-15	PhD	Civil Servant
P25	Male	Deputy Director	31-35	PhD	Civil Servant
P26	Male	Director	31-35	MSc	Civil Servant
P27	Male	Security expert	21-25	BSc	Consultant
P28	Male	Security expert	16-20	BSc	Consultant
P29	Male	Security expert	16-20	MSc	Consultant
P30	Male	Defence expert	21-25	PhD	Civil Servant
P31	Male	Security expert	31-35	PhD	Civil Servant
P32	Male	Security expert	21-25	BSc	Consultant
P33	Male	Pentester	16-20	BSc	Consultant
P34	Male	IT expert	31-35	MSc	Consultant
P35	Female	Deputy Director	21-25	MSc	Civil Servant

	Technical Expertise			Delphi Study		
Identifier	*General*	*Procurement*	*Security*	*Round 1*	*Round 2*	*Round 3*
P1	High	High	High	Yes	Yes	GT
P2	High	Medium	High	Yes	Yes	GT
P3	High	Low	High	No	Yes	GT
P4	Medium	High	Medium	Yes	Yes	GT
P5	High	Medium	High	Yes	Yes	GT
P6	High	High	High	No	Yes	GT
P7	High	High	Medium	No	Yes	GT
P8	High	High	Low	No	Yes	GT
P9	High	High	High	No	Yes	GT
P10	High	Medium	Low	No	Yes	GT
P11	High	High	Low	Yes	Yes	GT
P12	High	Medium	Medium	No	Yes	GT
P13	Low	High	Low	No	Yes	GT
P14	Medium	Medium	Medium	Yes	Yes	GT
P15	Medium	Medium	Medium	Yes	Yes	GT
P16	High	High	High	Yes	Yes	GT
P17	High	Medium	High	Yes	Yes	GT
P18	High	High	High	Yes	Yes	GT
P19	Medium	High	Low	Yes	Yes	GT
P20	High	Medium	High	No	Yes	GT
P21	High	High	High	No	Yes	GT
P22	High	High	Medium	Yes	Yes	GT
P23	High	High	Low	Yes	Yes	GT
P24	High	High	High	Yes	Yes	GT
P25	High	Medium	Low	No	Yes	GT
P26	High	High	Low	No	Yes	GT
P27	High	Medium	Medium	No	Yes	GT
P28	Low	High	Low	No	Yes	GT
P29	Medium	Medium	Medium	No	Yes	GT
P30	Medium	Medium	Medium	Yes	Yes	GT
P31	High	High	Low	No	Yes	GT
P32	High	Medium	Medium	No	Yes	GT
P33	Low	High	Low	Yes	No	GT
P34	Medium	Medium	Medium	Yes	No	GT
P35	Medium	Medium	Medium	Yes	No	GT

5.2.4 Data Collection and Analysis

The Delphi study took several months to complete, and consisted of three rounds of the Delphi study, as shown in Figure 5.1:

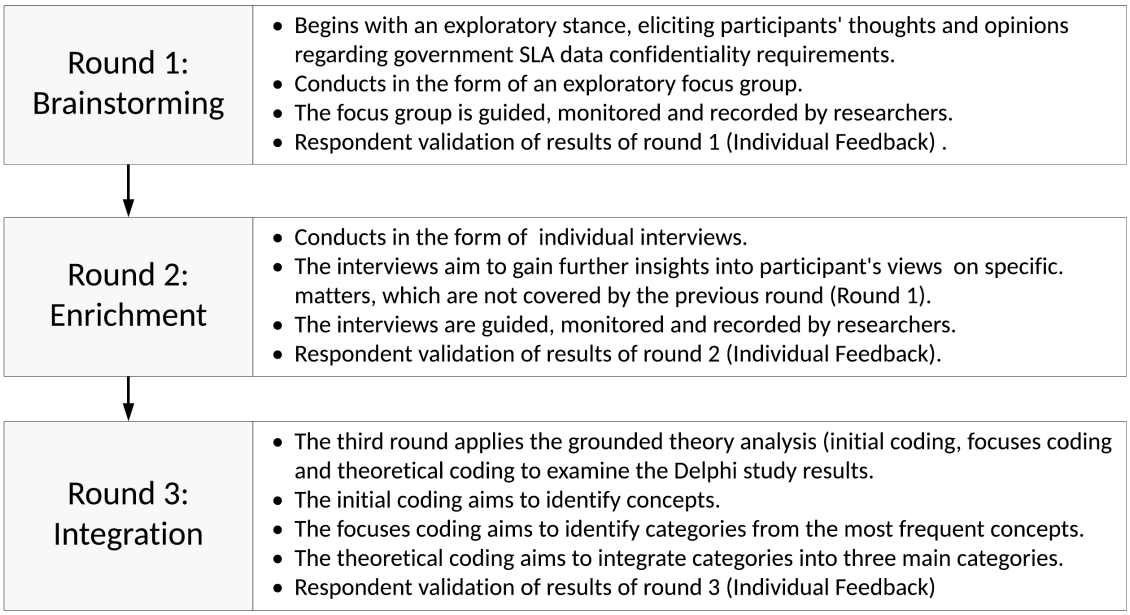


Figure 5.1: Phases of the Grounded Adaptive Delphi Method (GADM)

Round 1: Brainstorming Phase. The first step was the brainstorming phase through exploratory group discussions. A series of group discussions were conducted to allow participants to choose the appropriate time for participating in a group discussion. Each group discussed the problem of preserving the confidentiality of sensitive data across government agencies. Furthermore, participants were asked to explore Article 12 of the Government Regulation Number 82 of 2012, and how to incorporate the Government's data confidentiality requirements specified into SLA contexts.

In this round, 18 of 45 invited participants participated in three focus group discussions to explore a rich understanding of participants' experiences and opinions, and to generate information on collective views [135]. The optimum number of focus group members will vary between six to eleven [135]. However, in practice, a focus group can work successfully, with group members from three to fourteen participants [134]. For this chapter, focus group participants varied from three to six to allow participants to choose when to participate in a

group discussion. The initial transcripts of the first round were sent to participants to gather additional feedback and corrections if any.

Round 2: Enrichment Phase. This phase conducted an enrichment session using individual interviews to elicit detailed information from participants based on the results of the previous round. The initial transcripts of the first round and the Delphi questions which emerged were shared with 45 invited participants. The 45 participants were asked about their availability to participate in this study. The second round engaged with 32 participants and recorded each interview in an audio format after receiving the participant's consent. Each meeting took between 20-120 minutes. All Interviews were later transcribed and coded, and each transcription was sent to the interviewee for validation.

Round 3: Integration Phase. The third round applied the grounded theory analysis (initial coding, focus coding, and theoretical coding) [106–108] to examine the Delphi study data, and to categorise the extracted statements. The initial coding aimed to identify concepts from which the researcher extracted useful sentences or statements. The focuses coding aimed to identify and select categories from the most frequent or significant codes or concepts [108]. Once categories were identified, the theoretical coding aimed to integrate such categories into three increasing considerations of government's data confidentiality requirements in SLA definition. For a validation purpose, these findings were sent to each participant, who was asked for final feedback and corrections if any. The results of round 3 therefore constitute the final results of the GADM study.

5.3 Findings

This section presents the findings in three overarching themes: 1) target of protection; 2) risk perception; and 3) SLA data confidentiality requirements. These findings reveal opportunities for improving the consideration of the Government's data confidentiality requirements in SLA definition. By applying a grounded theory analysis, this chapter identifies emerging and essential concepts and categories present in the Delphi study data. These results are not quantitative; however, this study reports the raw number of participants who discussed a specific concept to give a rough indication of its prevalence amongst

participants. It is note that some participants failing to mention a particular concept does not necessarily mean that it is irrelevant to such participants. To illustrate how the results of this study were obtained, for example, one participant commented that 'the more significant threat to government agencies mostly come from internal sources, such as an insider threat'. This study coded it as *collaborator*, as described in Table 5.3.

5.3.1 Target of Protection

This study began by examining the Delphi study data from the perspective of what types of government assets to protect. Several concepts were discussed by participants related to sensitive government data and assets. Therefore, this chapter highlights concepts of target of protection, and consolidates the concepts into human assets, information assets and physical assets, as shown in Table 5.2.

Table 5.2: Target of Protection

Category	Concept	No. of Participants (of 35)
Human Asset	Protecting senior government officials	15
	Protecting knowledge and experience	2
	Protecting intellectual property	3
Information Asset	Protecting citizen data	13
	Protecting national identity	9
	Protecting health or medical records	13
	Protecting financial information	17
	Protecting military and defence data	25
	Protecting law enforcement data	10
	Protecting confidential diplomatic communications	4
	Protecting personal data and privacy	21
	Protecting intelligence data	7
	Protecting national economic interests	10
	Protecting natural and energy resources data	9
	Protecting tax information	6
	Protecting email communications	4
	Protecting state/government budget	3
Physical Asset	Protecting devices	4
	Protecting critical national infrastructure	5
	Protecting communication channel	2
	Protecting information systems	4
	Protecting government services	5

5.3.1.1 Human Asset

Many participants agreed that senior government officials were part of the target of protection. Many of the statements reported by participants were in line with the main category: *human assets*. The most common concept involved protecting upper-level government officials, such as president, vice president, ministers and deputy ministers, considered as target of protection.

Interestingly, participants reported that the Government has difficulty protecting government secrets against former senior officials. For example, some participants reported that many large corporations employed former officials with close ties to government agencies to gather their knowledge and experience. Therefore, this chapter emphasises discussions and opinions from government participants regarding the concepts of what types of government data and assets to protect related to human elements, such as the following:

> "*if the person is a senior official who carries out government duties, such person is subjected to be protected all the time because it is considered as an asset*" (P8).

> "*the secrets belong to government officials, such as a president can be uncovered by examining his/her previous unprotected information*" (P21).

5.3.1.2 Information Asset

The comments from the participants highlight that many government agencies routinely collect, create or process sensitive data as part of the delivery of public services. The majority of participants pointed out that the definition of sensitive data differed amongst government agencies. For example, each government ministry has different types of sensitive data that include health or medical information, financial data, military and defence data, law enforcement data, and citizen data. Many government assets discussed by participants were in line with the definition of sensitive government data. Therefore, participants expressed concern regarding protecting information assets that may not be appropriate for public release. For example, some representatives indicated the following:

"*every government agency is required to define sensitive data in their terms because the type of sensitive data in each agency differs with other agencies. For example, military and defence data protecting military and defence data*"(P1).

"*in some cases, the distinction between sensitive data and non-sensitive data looks "grey", for example, one has uploaded the entire government meetings including their internal meetings to social media, such as Youtube, with the aim to build trust to the public. However, some of the information should not be disclosed for public consumption, such as personal data and privacy*"(P2).

5.3.1.3 Physical Asset

Several participants (5 of 35) reported that the government's physical infrastructure and information systems had to be protected from threats which may result in exposure to liability. From a security perspective, participants focused on protecting physical assets, such as communication channels, systems and devices. In particular, participants considered the importance of protecting physical assets containing sensitive government data. Interestingly, several participants expressed concern about the importance of protecting physical assets, as important as the protection of information assets. For example, some representatives pointed out the following:

"*It is necessary to ensure adequate physical protection for information system facilities and infrastructures, such as data centre, networks, systems and devices protecting information systems*"(P12).

"*the need for protection of critical national infrastructure that has huge impacts on the human society, such as electricity and health facilities protecting critical national infrastructure*"(P29).

Overall, this chapter has identified 21 concepts within three main categories emerged from the Delphi study data. The three categories of the target of protection are, namely: 1) human asset; 2) information asset; and 3) physical asset. The findings have suggested that the

Government and its suppliers should handle sensitive government data with care and respect. However, the information obtained from the participants indicates that there is an absence of government security classifications applied to government agencies which generate, process, collect, store or transmit sensitive data for conducting government activities and delivering public services. Therefore, the Government should classify government data so that every entity which works with the Government knows how best to protect sensitive data, based the data classification and threat model.

5.3.2 Risk Perception

This subsection examines the perception of threats and risks to sensitive government data from unauthorised access. The participants of this study reported various security concerns and risks that the Government is attempting to counter. Some risk perception categories were raised during the investigation. Participants also mentioned several security risks that were not initially anticipated. For example, one participant discussed the possibility of impersonation attacks to obtain some confidential data. Some similar concepts emerged regarding the particular risk, and integrated into such categories of risk perception where applicable, as shown in Table 5.3.

5.3.2.1 Collaborator

Many participants (20 of 35) reported that insider threats were the most prominent risk perception factors in public administration. Such risk perception category allowed a malicious insider to cooperate traitorously with an adversary. Therefore, the participants of this study paid much attention to mitigating insider threats. One participant highlighted that government data leakage was mainly caused by an insider who was a closely related person with senior officials, as follows:

> "*the issue of sensitive government data theft normally does not occur while data is transmitted, but when data was processed or created. While having a discussion with...an insider can listen and participate in the discussions and then disclose and share the information obtained with an adversary*" (P22).

Table 5.3: Risk Perception

Category	Concept	No. of Participants (of 35)
Collaborator	Identifying insider threats by employees	13
	Identifying insider threats by contractors	2
	Identifying insider threats by service providers	2
	Identifying insider threats by government partners	3
Exfiltration	Identifying outbound traffic	3
	Identifying key exfiltration by a service provider	4
	Identifying content exfiltration by a service provider	3
	Identifying data exfiltration by malware	2
	Identifying data exfiltration by connected devices	2
Observation	Identifying interception (content/traffic)	15
	Identifying discovery by foreign governments	7
	Identifying metadata collection by foreign agencies	4
Insertion	Identifying a malware injection (trojan/backdoor)	17
	Identifying a ransomware installation	3
Manipulation	Identifying phishing attacks	7
	Identifying social engineering attacks	8
	Identifying impersonation attacks	1

The statement above was coded as the concept of identifying an insider threat by an employee. The concept is categorised as *collaborator*. Another two participants (2 of 35) discussed insider threats from service providers, for example, P29 noted the following statement:

> "*service providers have a better understanding of how to gain access to resources, such as data centres that store confidential data*" (P29).

5.3.2.2 Exfiltration

Many participants (14 of 35) were concerned with the illegal copying or transfer of sensitive data through various means. Participants reported that such threats allowed an adversary to perform the unauthorised copying, transmission or retrieval of sensitive data from the government's information systems. P13, who worked as a government consultant, indicated the following:

"*There is a threat, which we consider before the threat was always from the outside, so we then place a firewall, intrusion detection, and so forth. But the fact that now the threats and attacks actually come from inside...according to our observation, we discovered botnets keep sending out information*" (P13).

The statement above was coded as the concept of identifying outbound traffic. The concept is categorised as *exfiltration*. As another example, several participants (3 of 35) discussed content exfiltration by a service provider. P18 noted the following statement:

"*the service provider should provide explicit guarantees regarding the security of the data it manages. How the service provider secures the data, as required should be explained to the customer. Then, the need for a monitoring system to ensure that the data is not transferred or copied to unauthorised parties*" (P18).

5.3.2.3 Observation

Many participants (15 of 35) discussed the importance of securing communications against interception by third parties. Most government employees including senior government officials typically transfer sensitive government data using phones, emails, SMS or in person with limited use of encryption. Some participants reported that some senior officials preferred meeting in person for transferring the most sensitive information.

Further, several participants (7 of 35) mentioned concern about being surveillance targets by foreign intelligence services, while a few participants (4 of 35) expressed concerns about bulk metadata collection and access by such foreign intelligence agencies. Overall, the participants reported the importance of preventing observation by well-funded adversaries, as this threat allowed the adversary to observe or monitor targets closely. Some representative participants indicated this type of risk, as follows:

"*we should be aware that when we are talking with our interlocutor, other people are listening to our communications without knowing them*"(P4).

"*the most in need of government secrets is foreign intelligence agencies. They need such information for their purposes*"(P29).

5.3.2.4 Insertion

Many participants (17 of 35) reported that malicious software (malware) injection could steal sensitive data, like credit card numbers, healthcare records or classified military plans. The participants discussed that such an adversary model could place or insert malware on the targeted government's information systems through various methods, as indicated in the following statement:

> "*they embed code on the opposing side in any way to divulge the sensitive government data*" (P1).

The statement above was coded as the concept of identifying a malware injection (trojan or backdoor). The concept is categorised as *insertion*. As another example, a few participants (3 of 35) discussed a ransomware attack through government information systems. P14 noted the following statement:

> "*An example of a case that it occurred in one agency which administers the national health insurance, which was attacked by malware where all the data on the server was encrypted*" (P14).

5.3.2.5 Manipulation

The participants of this study expressed concern about phishing, spear phishing, social engineering or impersonation attacks. Participants reported that the action of manipulating information systems was a common way to obtain sensitive data from targets (e.g. people). Such threats allow an adversary to pretend to be another person with the aim of collecting sensitive government data from the target. For example, P3 pointed out the following statement.

> "*for threats to military information and sensitive government data, in general, the threats were in the form of impersonation. Besides the impersonation, they could also do phishing*" (P3).

The statement above was coded as the concept of identifying impersonation attacks. The concept is categorised as *manipulation*. As another example, the participants discussed phishing and social engineering attacks. P15 noted the following statement:

"*Email and web are such vectors for delivering phishing attacks because both vectors are frequently accessed via mobile and desktop*" (P15).

In short, this subsection has identified 17 concepts within five main categories that emerged from the Delphi study data. The five categories of risk perception are, namely: 1) collaborator; 2) exfiltration; 3) observation; 4) insertion, and 5) manipulation. The categories of risk perception which emerged in this study can be performed by hackers, insiders, and advanced persistent threat (APT) or state-sponsored attacks. However, such adversary models are not necessarily exclusive. However, the categories of risk perception can be applied to an area preserving the confidentiality of sensitive government data against unauthorised access. In so doing, it is of paramount importance to define government SLA data confidentiality requirements according to perceived risks to sensitive government data.

5.3.3 SLA Data Confidentiality Requirements

This subsection introduces understandings of the concepts related to the government SLA data confidentiality requirements. As such, by identifying the specific characteristics of threats and risks against unauthorised access to sensitive government data, the concepts of SLA data confidentiality requirements were developed from the data analysis. In this chapter, some concepts of SLA data confidentiality requirements were expressed by participants, and consolidated into categories of the government SLA data confidentiality requirements where applicable, as shown in Table 5.4. It is note that when government agencies procure external information system services from external service providers, it is necessary to incorporate the Government's data confidentiality requirements into SLAs.

5.3.3.1 Access Management

Many participants (17 of 35) discussed having secure communications, particularly for transferring sensitive government data. Participants reported that the importance of securing communications was to prevent eavesdropping and data leakage during transmission of sensitive government data. Interestingly, participants mentioned that protecting the integrity

Table 5.4: Understanding of SLA Data Confidentiality Requirements

Category	Concept	No of Participants (of 35)
Access Management	Requiring secure communications	17
	Requiring access control to sensitive data	13
	Requiring limited access to sensitive data and assets	18
	Requiring isolation from unaurhorised access	18
	Requiring zero-knowledge access controls	5
Data Management	Requiring encrypting data during transmission	19
	Requiring encrypting data during storage	14
	Requiring encrypting data during processing	2
	Requiring key management	5
	Requiring adequate data classification controls	22
	Requiring data sharing controls	8
Identity Management	Requiring privileges to access sensitive data	2
	Requiring single-factor authentication	7
	Requiring multi-factor authentication	7
	Requiring strong authentication	1
	Requiring log files and access control lists	3
Malicious Management	Requiring appropriate personnel security screening	3
	Requiring data leakage monitoring	5
	Requiring physical security	15
	Requiring risk assessment	27
Compliance Management	Requiring certification and attestation of suppliers	4
	Requiring compliance with standards and regulations	12
	Requiring compliance with data location requirements	3
	Requiring compliance with in-house rules	3

of government data transmitted over a network was also necessary. For instance, P10 reported relatively strong support for securing communications, as described by the following statement:

> "*In the future, we should require every employee in government agencies to have a public key and a secret key when communicating through government email services because the content of email communications and its metadata needs to be protected*" (P10).

Another participant reported that network communications were necessary to be controlled and secure against threats, as follows:

> "*we need to think secure government networks with a single entrance point, so if there is a leak, we can know from which point*"(P1).

The two statements above were coded as the concept of requiring secure communications. The concept is categorised as *access management*. As another example, participants discussed requiring access control as a means of controlling or limiting access to sensitive government data. P8 noted the following statement:

> "*It is important to allow who is entitled to access the data. However, authentication is required to enter the systems*" (P8).

Further, participants reported that access control was required to ensure that all sensitive government data were limited to authorised users. P15 noted the following statement:

> "*Who gets access to the information systems? A trusted person must need approval first before directly go into the system*" (P15).

5.3.3.2 Data Management

Many participants discussed the importance of encrypting sensitive government data during transmission and storage. Most commonly, the participants of this study mentioned using encryption to protect communications or stored data, while few participants expressed concerns protecting sensitive data and communications during processing. P19 reported the following statement:

> "*As an example, the secret communications between the Ambassador and the Ministry of Foreign Affairs. The line of communication has been secured using secure channels. When both parties receive information, the information is stored in a secure storage facility. However, when the process of making such information there is no way to protect the data during processing*" (P19).

The statement above was coded as the concept of requiring encrypting data during transmission, storage or processing. The concept is categorised as *data management*. As another example, the majority of participants (22 of 35) expressed concerns on requiring adequate data classification controls as a means of protecting sensitive government data with appropriate security levels. P6 noted the following statement:

"*The need for security requirements to protect sensitive data based on the level of confidentiality, including secrets and top secrets so that appropriate controls can be implemented to protect government data at each classification*" (P6).

5.3.3.3 Identity Management

Many government SLA data confidentiality requirements reported by participants were in line with authentication and authorisation. The most common requirements involved requiring authentication and privileges to access sensitive data. Participants also mentioned several requirements including requiring log files and access control list. Two representative participants described confidentiality requirements for allowing access to the systems:

"*To access government secrets- information of interest to nation states, it requires a combination of four of the seven senior government employees who hold passwords to access such sensitive information*" (P21).

"*such access will be provided by needs and job descriptions so that such person can not access all government information systems*" (P26).

The two statements above were coded as the concept of requiring multi-factor authentication and requiring privileges to access sensitive data. Such concepts are categorised as *identity management*. As another example, one participant expressed concerns about how to protect sensitive government data (the secrecy, integrity and availability of sensitive data) when using external information system services. P3 pointed out the following statement:

"*government requirements should not allow sensitive government data to store in other countries without additional security capabilities taken, such as a strong authentication*" (P3).

5.3.3.4 Malicious Management

The majority of participants (27 of 35) discussed the importance of requiring risk assessment when using external information system services provided by external service providers. Another majority requirement reported by participants was physical security. While a few participants expressed concerns about personal security screening and data leakage monitoring, participants expressed concern about people as a point of security failure. Such concepts were categorised as *malicious management*. For example, one participant mentioned physical security measures as described in the following statement:

> "*it seems that security controls should be integrated with physical elements, such as a room, doors and locks that need to be installed*" (P32).

Another participant also mentioned physical security as described in the following statement.

> "*Security screening and access control list should exist. Such access restriction is implemented based on a need-to-know basis*" (P6).

5.3.3.5 Compliance Management

Many participants (12 of 35) discussed the importance of requiring compliance with standards and regulations when procuring external information system services provided by external service providers. For example, two representative participants reported the following statements:

> "*The business process applied constantly considers the security aspect of preserving the confidentiality of sensitive data, and they must ensure that all business processes are compliant with security standards and best practices*" (P12).

> "*For example, when procuring government services, technical specifications should be submitted by the prospective suppliers to check whether or not comply with the required security requirements*" (P30).

Additionally, several participants (4 of 35) expressed concern about trustworthiness of suppliers or service providers through certification schemes, such as ISO/IEC 27001. P23 reported the following statement:

> "*By applicable regulations, electronic system operators, who handle public sectors, are divided into three categories of impact namely low, high, and critical. Both high and critical categories are required to have ISO/IEC 27001 certification with additional controls for a critical category*" (P23).

While a few participants discussed having data localisation requirements, particularly for sensitive information, they did not elaborate on the technical considerations to address such requirements. Practically, participants referred to existing laws and provisions which require any organisation who handle public sectors to store their data under Indonesian jurisdiction. For example, P7 reported the following statement:

> "*No one knows better than the Central Bank of Indonesia or the Financial Services Authority concerning confidential information from bank customers. They know better and establish how the data will be protected. Such data must be encrypted; must be transferred through a secure line, and should not pass through international connections, and the data centre must be located in Indonesia*" (P7).

Interestingly, several participants mentioned explicit requirements for building trust through the use of local providers and products to handle the most sensitive information. For example, P1 noted the following statement:

> "*For protecting the secret and top-secret information, all encryption keys are a local production. Additionally, local providers are necessary to provide secure network services, such as virtual private network services*" (P1).

In conclusion, this subsection has identified and described 22 concepts within five main categories which emerged from the Delphi study data. The five categories of government SLA confidentiality requirements, namely: 1) access management; 2) data management; 3)

identity management; 4) malicious management; and 5) trust and compliance management. The findings indicate that participants reveal undeveloped government SLA confidentiality requirements. The preference for the SLA confidentiality requirements is evident even though there will be room for improvement to incorporate such confidentiality requirements into SLA definitions.

5.4 Discussion

This section compares the findings of this study with extant literature to confirm or contradict the obtained results, and elaborates on the implications of the findings for the government and make concrete recommendations for how the findings can be used to guide the development of a TDSLA capability framework.

5.4.1 Reflection on related works

As discussed in Chapter 2, the UK government introduces Cyber Essentials (CE) [59], which can serve as an assurance scheme for external service providers who want to conduct business with the government agencies and public sector organisations. The CE requirements are identified to mitigate common successful cyber-attacks, such as malware, phishing, and unpatched software in such an organisation. The five primary security requirements are: boundary firewalls and Internet gateway; secure configurations; user access control; malware protection; and patch management. Compared to the CE requirements, the findings of this chapter is designed to investigate the perception of government SLA confidentiality requirements for the context of the Indonesian government. Additionally, the study is concerned with the investigation of the Government's data confidentiality requirements, not broadly security requirements.

The UK government also outlines 14 cloud security principles [62], namely: data in transit protection; asset protection and resilience; separation between customers; governance framework; operational security; personnel security; secure development; supply chain security; secure customer management; identity and authentication; external interface protection; secure service administration; audit information provision to customer; and

secure use of the service. Such principles are used by UK government agencies who want to procure cloud-based services from external service providers. Again, this chapter focuses on an understanding of the Government's data confidentiality requirements that can be incorporated into the new definition of SLAs through an appropriate discrete level of assurance. Each level has a different level of SLA data confidentiality requirements. It is apparent that the findings of this chapter can be applied to various service scenarios such as cloud-based services.

In the context of the US government procurement policy, any potential and existing suppliers, service providers or contractors working with the federal agencies are required to meet 14 confidentiality requirements described in the NIST standard SP800-171 [47, 60]. Such requirements are, namely: access control; awareness and training; audit and accountability; configuration management; identification and authentication; incident response; maintenance; media protection; personnel security; physical protection; risk assessment; security assessment; system and communications protection; and system and information integrity. Although such guidelines are mainly concerned with the protection of the confidentiality of controlled unclassified information when using external information system services from external service providers, the confidentiality requirements are not directly applicable to SLAs in general. As such, this chapter aims to increase the consideration of the Government's data confidentiality requirements in SLA definitions.

In other work, Takahashi et al. [35] classify the target of protection into three main themes: people; information; and physical asset. Such themes are in line with the findings of the study. As the findings emerged from the data, it is essential to compare the findings of this study with extant literature to validate such findings. Moreover, Barnes et al. [53] introduce confidentiality threat model into six attacker capabilities: passive observation; passive inference; active; static key exfiltration; dynamic key exfiltration; and content exfiltration. These categories are in line with the five categories of confidentiality risk perception that emerged from the Delphi study data.

Furthermore, Singh et al. [163] identify and describe 20 security considerations for cloud-supported Internet of Things within the following categories: data transport to/from cloud services and data management; identity management; managing scale for the IoT-Cloud;

malicious things; certification, trust and compliance with regulations and contractual obligations; and decentralised clouds. Although such security considerations are not justifiable in the context of the Indonesian government, all security considerations also focus on ensuring the confidentiality of data, except one security consideration of an increase in interaction and data load. Compared to the work of Singh et al. [163], the findings of this chapter developed from the Delphi study data. Even so, the five main categories of government SLA confidentiality requirements are in line with the extant literature [163], namely: 1) access management; 2) data management; 3) identity management; 4) malicious management; and 5) compliance management. In essence, it is necessary to examine the extant literature with the concepts and categories that emerged from the data, as Charmaz [108] highlights the need to tailor a literature review to fit the aim of the grounded theory study.

5.4.2 Main Outcome

From the perspective of the government participants, this chapter considers the following takeaways to be the most important ones from the findings:

- The perception of the target of protection is correlated with the categories of human assets, information assets and physical assets. Particularly for information assets, all government data has value and should be classified. It is important to note that any entity who handles sensitive government data must adhere to a duty of confidentiality according to the data classification and threat model. Access to sensitive data should only be granted on a need-to-know basis. Additionally, any information exchanged should receive the same protection from unauthorised access. Thus, an appropriate level of security assurance must be formulated and incorporated into the form of SLAs, based the data classification and threat model.

- The perceptions of data confidentiality risks are correlated with five categories of threat models, such as collaborator, exfiltration, observation, insertion and manipulation. However, it is nontrivial to classify such risk perceptions or threat models into security classifications and discrete levels of assurance. Thus, it is essential to understand actual threat capabilities by enriching the expressiveness of threat model statements.

- The perception of government SLA data confidentiality requirements is correlated with the categories of access management, data management, identity management, malicious management, and compliance management. However, the Government needs to elaborate these confidentiality considerations into standard government SLA data confidentiality requirements. As such, it increases the considerations of the Government's data confidentiality requirements in SLA definitions.

5.4.3 Recommendations

The findings raised by this chapter indicate recommendations for government agencies, service providers and researchers, as follows:

- **Implications for government agencies**. The findings of this study suggest that the Government should ensure the protection of sensitive government data and assets, whether it is stored in an electronic or paper format. For an electronic form, whether sensitive data is stored in cloud storage systems, on mobile devices, on portable storage devices or laptop or desktop computers. Indeed, each sensitive government data is in keeping with unique confidentiality requirements based the data classification and threat model. Further, understanding data confidentiality risks to sensitive government data are necessary. The findings of this study identify specific threats and risks, which are scattered across various participants. Therefore, the Government should identify which perceived threats and risks are mitigated best by data confidentiality capabilities offered by service providers.

- **Implications for service providers**. The statements from participants identify that government agencies commonly make decisions to protect government data by applying specific security capabilities through technical, physical and human elements of information security. In this case, government agencies heavily rely on certification schemes, such as ISO/IEC 27001, which is not sufficient to address specific perceived and emerging threats [15]. While in some cases government agencies do not provide high-level data confidentiality requirements up-front, external service

providers should consider appropriate security controls for protecting sensitive government data. In either case, the Government should understand what categories of data confidentiality requirements that need to be defined in SLA contexts. By doing so, service providers can determine and negotiate appropriate data confidentiality capabilities, which demonstrate compliance with the Government's data confidentiality requirements. Therefore, the level of trust between government agencies and service providers can be determined by using service provision for data confidentiality provided by service providers.

- **Implications for researchers**. The findings of this study provide a rich foundation for incorporating the interplay of the target of protection, perceived risks and data confidentiality requirements specified in SLA contexts. However, it is difficult to negotiate explicit contractual terms about the required data confidentiality requirements and the available confidentiality capabilities regarding the data classification and risk level. Often, there is the risk of liability and compensation with the particular level of security expressed in SLAs. These questions sketch many avenues for future work.

5.5 Chapter Summary

This chapter has investigated understandings of government SLA data confidentiality requirements for the context of the Indonesian Government. In this investigation, the section set out to provide some insights into three understandings of increasing considerations of the Government's data confidentiality requirements in SLA definitions. The three perceptions of security-related SLAs are namely: 1) the perception of the target of protection; 2) the perception of the data confidentiality risks; and 3) the perception of the government SLA data confidentiality requirements. The findings of this study are in line with the extant literature. As the findings emerged from the data, it is essential to compare such findings (concepts and categories) with related works.

Further, the findings of this chapter indicate that the government SLA confidentiality requirements have seen limited demand for service provisions in government contracts relating to external information system services supplied by external service providers.

The Government SLA data confidentiality requirements that emerged from this study are, namely: 1) access management; 2) data management; 3) identity management; 4) malicious management; and 5) compliance management. The evidence from this chapter suggests that there is a need for an approach to incorporate data confidentiality capabilities specified in SLA contexts to enhance the level of trust and security in a service provisioning environment, such as cloud-based services between government agencies and external service providers. Therefore, further research needs to examine service provision for confidentiality in real-world SLAs between government agencies and services providers. The following chapter investigates the perception of service provision for data confidentiality in SLA contexts by studying external service providers that provide external information system services to the Government of Indonesia.

6

Service Provision for Data Confidentiality in Service Level Agreements

> *It is important to have a fairly clear understanding of what you are looking for and what events you are interested in because you cannot collect or detect everything.*
>
> Stephen Northcutt, *President of the SANS Technology Institute*, 1999

Chapter 6 draws on refereed articles described in the following publications:

- Y. Nugraha and A. Martin. Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments. In: Steghöfer JP., Esfandiari B. (eds) Trust Management XI. IFIPTM 2017. IFIP Advances in Information and Communication Technology, vol 505, pp.57-75, Springer, Cham, 2017 [13].
- Y. Nugraha and A. Martin. A Study Investigating Service Provision for Data Confidentiality in Service Level Agreements: An Indonesian Government Case Study. This manuscript is in the process of submission to a journal publication.

Contents

6.1 Introduction

Many governments prefer to procure and use external information system services, such as cloud services to store government data [58, 164]. For example, the UK Government issues the 'Government Cloud First Policy' which mandates that UK government agencies and public organisations should consider cloud services first before considering any other solution when procuring services [165]. Instead of buying hardware, software and storage, government agencies have to manage service contracts with external service providers. Although Government's use of cloud service focuses on the system availability rather than data confidentiality, it is worthwhile to investigate whether existing SLAs could be adequate for addressing the levels of security for services that handle sensitive government data.

This situation above is in line with Article 12 of the Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012 which requires service providers to have agreements on minimum service level and information security when provisioning such external services to customers including government agencies. However, the concept of SLAs for security service provisions is relatively new to government agencies and service providers, and security service provisions related to data confidentiality are not well-established.

Previous studies have reported that the SLAs implemented by external service providers are based on provisions that can be measured, such as service availability, throughput, response times, resolution times, charging rate and penalties [33, 34, 96, 98]. However, data security (data confidentiality, data integrity and data availability) is often overlooked when expressing such provisions in SLAs [33, 34] because many service providers rely on certification schemes to guarantee the security of services offered to customers. As the previous chapter indicates, there is a need to increase the consideration of the Government's data confidentiality requirements in SLA definitions. The chapter has investigated the perceptions of government SLA data confidentiality requirements for the context of the Government of Indonesia. It is apparent that the use of assurance-based SLAs is becoming increasingly crucial in suppliers' relationships when government agencies procure and use such external information system services from external service providers.

This chapter examines the current provisions of SLAs offered by service providers to government agencies and identifies possible provisions for data confidentiality in SLA contexts. As such, this chapter conducted a longitudinal study of the Government's auctions of 59 e-procurement services across 80 Indonesian government agencies between 2010 and 2016 to select major service providers that provided Internet services, cloud-based services and data centre services. The chosen service providers were then contacted to participate in this study through the GADM method with 15 participants from selected service providers, with group discussions and individual feedback to investigate existing provisions of SLAs offered by service providers to government agencies, and to explore possible provisions for data confidentiality in SLAs. The data collection and analysis were conducted in three phases: 1) a brainstorming phase; 2) an enrichment phase; and 3) an integration phase.

Based on the findings of the Delphi study data, this chapter synthesises findings into three central themes: 1) risk perception; 2) current provisions of SLAs; and 3) possible provisions for data confidentiality in SLAs. This study reveals that government agencies rely on the experience of service providers in implementing appropriate security controls to protect sensitive government data against a range of applicable threats and risks. Additionally, this study found that the ISO/IEC *27001* certification was paramount for assuring government agencies about the quality of protection provided when handling government data and services. In other words, both government agencies and services providers rely on the ISO/IEC *27001* certification to provide security assurance in service provisioning. However, such assurance-based certification is not suitable for service provisioning. Therefore, there is a need to enhance the role of SLAs for data confidentiality in service providers' relationships. In essence, it is necessary to incorporate the Government's data confidentiality requirements into SLA contexts to reach and guarantee a discrete level of security assurance that can satisfy the real government needs and requirements.

The remainder of this chapter is structured as follows. Section 6.2 describes the method used in conducting the study including service provider selection, recruitment and data collection and analysis. Section 6.3 presents the results of the study. Section 6.4 discusses how the findings compare with related work, and elaborates on the implications of the findings for concrete recommendations. Section 6.5 summarises the chapter.

6.2 Method

6.2.1 Aim

This chapter investigates the current provisions of SLAs offered by service providers to government agencies, and identifies possible provisions of security services against unauthorised access to sensitive government data that are being processed, stored and transmitted by external information system services. Notably, the chapter examines existing real-world SLAs offered by selected service providers to Indonesian government agencies.

A significant impetus for this research emerged from Article 12 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012. The Government Regulation states that service providers are required to have agreements on minimum service level and information security when providing such external services to customers including government agencies. Although SLAs can be established with various interacting entities (i.e. customers, end-users, service providers, suppliers, integrators, standards bodies and accreditation bodies), the scope of the study is limited to government agencies that procure such external services from external service providers.

In this chapter, the research activities conducted in a five-phase of data collection and analysis, namely: 1) a longitudinal study of the government auctions for service provider selection; 2) recruitment; 3) a brainstorming phase with several group discussions; 4) an enrichment phase through several more group discussions; and 5) an integration phase using grounded theory analysis (initial coding, focused coding and theoretical coding) of the Delphi study data to categorise the statements from participants [106–108].

6.2.2 Service Provider Selection

This study conducted a longitudinal study of the government auctions of 59 e-procurement services across the 80 Indonesian government agencies between 2010 and 2016 to select major service providers that provided Internet services, cloud-based services and data centre services. This work defines a longitudinal study as one in which each government auction for such services is observed on more than one occasion [166]. The longitudinal study was

designed to increase the precision of selecting service providers as well as to identify the winners of government auctions each financial year from 2010 to 2016.

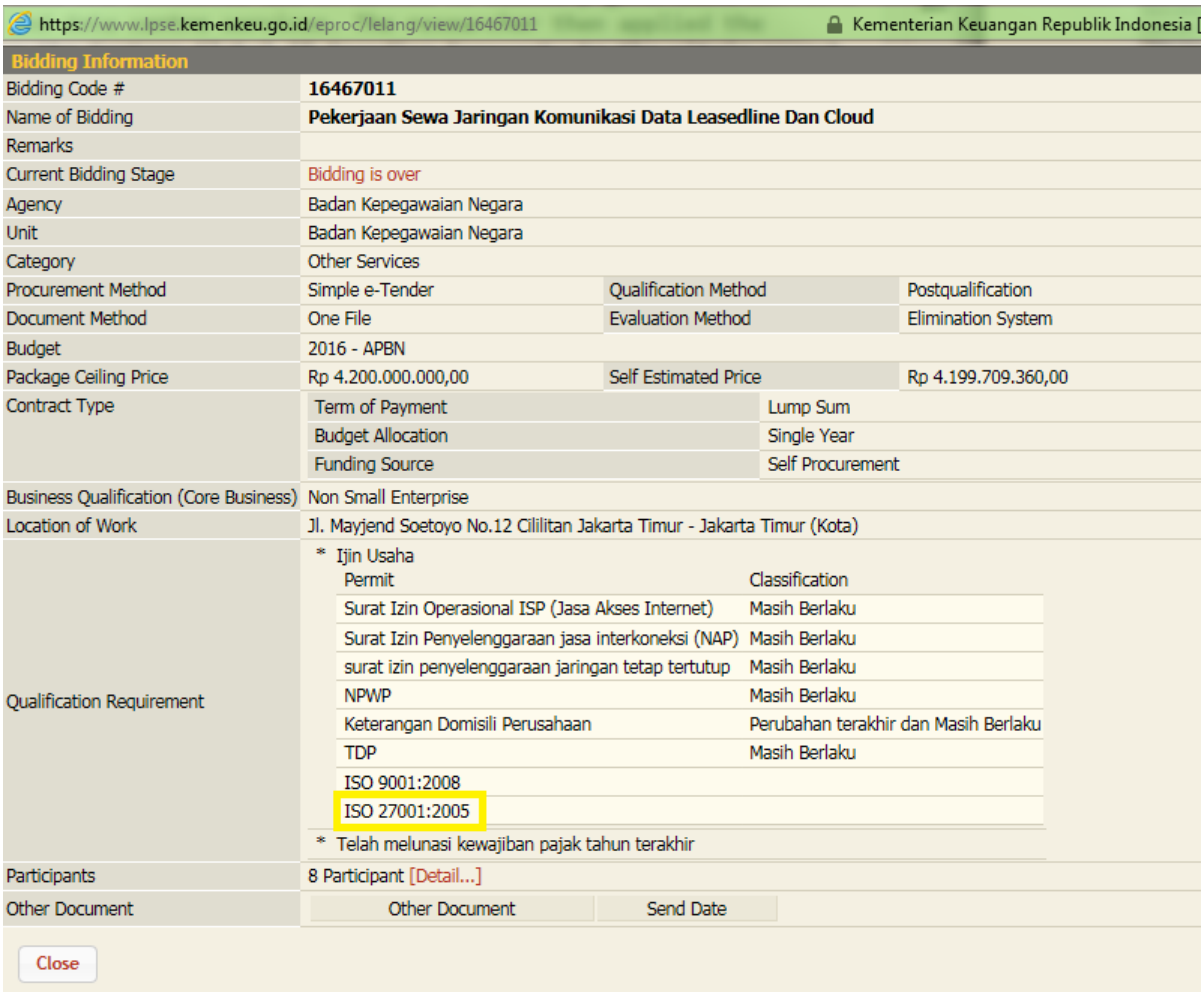
The data collection was conducted from March 2016 to July 2016 and carried out the search process in the following steps.

Step 1—The researcher accessed the procurement service website for each government agency. Some agencies engaged with other procurement services from other agencies. Most of the procurement service website follow the general format: `lpse.[goverment agency's website]/eproc/lelang]`, for example `lpse.kemenkeu.go.id/eproc/lelang`. From 2010 to 2016, `95944` government auctions were found across 59 procurement services websites.

Step 2—The researcher used the automated search method to classify government auctions regarding the Internet services, cloud-based services and data centre services. The researcher then applied the following *five* keywords, which were adopted from the Gartner Global IT Spending Forecast, to the site's search engine: 1) **Data Centre**; 2) **Cloud**; 3) **Co-location**; 4) **Internet**; and 5) **Network**). By reading the title of government auctions as well as identifying the relevant keywords, the researcher extracted **273** government auctions for data centre category, **31** government auctions for cloud category, **17** government auctions for co-location category, **230** government auctions for Internet category and **236** government auctions for network category, as shown in Table 6.6.

Step 3—The researcher examined each government auction that aimed to retrieve government requirements for selecting external service providers as shown in Figure 6.1.

Step 4—Finally, the researcher identified the winning bidder, as shown in Figure 6.2. The selected service providers were then identified according to the number of bids won and the value of the procurement project handled by service providers. This process is a rationale for selecting the selected service providers; and lastly, five selected major services providers were identified as the winners of government auctions, as shown in Table 6.7.



https://www.lpse.kemenkeu.go.id/eproc/lelang/view/16467011 — Kementerian Keuangan Republik Indonesia

Bidding Information

Bidding Code #	**16467011**		
Name of Bidding	**Pekerjaan Sewa Jaringan Komunikasi Data Leasedline Dan Cloud**		
Remarks			
Current Bidding Stage	Bidding is over		
Agency	Badan Kepegawaian Negara		
Unit	Badan Kepegawaian Negara		
Category	Other Services		
Procurement Method	Simple e-Tender	Qualification Method	Postqualification
Document Method	One File	Evaluation Method	Elimination System
Budget	2016 - APBN		
Package Ceiling Price	Rp 4.200.000.000,00	Self Estimated Price	Rp 4.199.709.360,00
Contract Type	Term of Payment	Lump Sum	
	Budget Allocation	Single Year	
	Funding Source	Self Procurement	
Business Qualification (Core Business)	Non Small Enterprise		
Location of Work	Jl. Mayjend Soetoyo No.12 Cililitan Jakarta Timur - Jakarta Timur (Kota)		

Qualification Requirement

* Ijin Usaha

Permit	Classification
Surat Izin Operasional ISP (Jasa Akses Internet)	Masih Berlaku
Surat Izin Penyelenggaraan jasa interkoneksi (NAP)	Masih Berlaku
surat izin penyelenggaraan jaringan tetap tertutup	Masih Berlaku
NPWP	Masih Berlaku
Keterangan Domisili Perusahaan	Perubahan terakhir dan Masih Berlaku
TDP	Masih Berlaku
ISO 9001:2008	
ISO 27001:2005	

* Telah melunasi kewajiban pajak tahun terakhir

Participants	8 Participant [Detail...]		
Other Document	Other Document	Send Date	

Close

Figure 6.1: Government Auction Information

https://www.lpse.kemenkeu.go.id/eproc/rekanan/lelangpeserta/16467011 — Kementerian Keuangan Republik Indonesia

Evaluation result

No	Participant Name	Administration	Technical	Bid price	Evaluated Price	Winner	Justification
1	PT. Indonesia Super Corridor - 02.699.198.4-014.000						
2	PT.Platinum Network Indonesia - 02.143.542.5-064.000						
3	PT Telekomunikasi Indonesia Tbk - 01.000.013.1-093.000	✔	✔	Rp 4.107.319.920,00	Rp 4.107.319.920,00	☆	Memenuhi syaratMemenuhi syaratMemenuhi syarat kewajaran harga
4	PT Mora Telematika Indonesia - 01.973.886.3-007.000						
5	PT Aplikanusa Lintasarta - 01.329.929.2-092.000						
6	PT. CYBER NETWORK INDONESIA - 02.427.219.7-014.000	✔					Memenuhi syaratTidak memenuhi syarat
7	PT. Palapa Network Nusantara - 02.699.196.8-014.000						
8	Jasa Jejaring Wasantara - 01.732.837.8-031.000						

Figure 6.2: Auction Winner

6.2.3 Recruitment

After identifying the selected major service providers that provided cloud-based services, data centre services and infrastructure services to government agencies, this study invited the five primary service providers through an official invitation letter signed by a senior official who was the head of the department that administers cyber security and information assurance in Indonesia. The five selected service providers were chosen based on the fact that they were auction winners for government tenders for services, as shown in Table 6.7. The official letters including participant sheets and consent forms were then sent to each service provider through senior management.

After receiving a confirmation from each management, participants from each company were proposed according to the following the selection criteria: 1) work experience and background; 2) involvement in the government procurement auctions; and 3) a visible interest in the research topic. Finally, 15 participants [P1–P15], who were representatives from the five selected service providers, were confirmed to take part in this study. Representative participants were technical and regulatory compliance experts across the spectrum of general technical, procurement and security expertise. Such participants have been working for many years in each company or service provider (`SP`) {`SP1`, `SP2`, `SP3`, `SP4`, `SP5`} that provided Internet services, cloud-based services and data centre services to the Indonesian government agencies. The details of companies are not provided, to respect assurance of anonymity of the participants.

6.2.4 Procedure

All data collection and analysis activities were conducted from July 2016 to January 2017. Each group interview or group discussion was audio recorded and later transcribed and coded using grounded theory analysis. Each group discussion within the Delphi study took between 60 - 120 minutes. For each round of Delphi, participants were asked to respond to the following questions:

Part 1: General. Participants were asked to tell about the service provider's compliance with Article 12 of the Indonesian Government Regulation on the Operation of Electronic

Table 6.1: Participants' Information and Experience

			Participant	
Identifier	*Gender*	*Role*	*Years' Experience*	*Service Provider*
P1	Female	Manager	11-15	SP1
P2	Male	Vice President	16-20	SP1
P3	Male	Specialist	6-10	SP1
P4	Male	Manager	16-20	SP2
P5	Male	Specialist	6-10	SP2
P6	Male	Specialist	6-10	SP2
P7	Male	Manager	16-20	SP3
P8	Male	Specialist	6-10	SP3
P9	Male	Specialist	6-10	SP3
P10	Male	Manager	16-20	SP4
P11	Male	Manager	16-20	SP4
P12	Male	Specialist	6-10	SP5
P13	Male	Legal Officer	6-10	SP5
P14	Male	Manager	16-20	SP5
P15	Male	Manager	16-20	SP5

		Technical Expertise	**Data Collection**		
General	*Procurement*	*Security*	*R1-A*	*R1-B*	*R2*
High	High	High	No	Yes	Yes
High	Medium	High	No	No	Yes
High	High	High	No	Yes	Yes
Medium	High	Low	Yes	Yes	Yes
High	Medium	High	Yes	Yes	Yes
High	High	High	No	No	Yes
High	High	Medium	Yes	No	No
High	High	Low	Yes	No	No
High	High	High	Yes	Yes	No
High	Medium	Low	Yes	Yes	Yes
High	High	Low	Yes	Yes	Yes
High	Medium	Medium	Yes	Yes	Yes
Low	High	Low	Yes	Yes	No
Medium	Medium	Medium	Yes	No	No
Medium	Medium	Medium	Yes	No	No

Systems and Transactions Number 82 of 2012. The Government Regulation requires a service provider to have agreements on minimum service level and information security when provisioning services to customers. In this context, participants were asked about:

- Whether the service provider had compliance with the Government Regulation;
- Whether the service provider offered specific provisions for data confidentiality to government agencies; and
- Whether the service provider incorporated specific provisions for data confidentiality into SLA contexts.

Part 2: The Current Provisions of SLAs. Participants were asked to tell about the service provider's capabilities. In this context, participants were asked about:

- What the current provisions of SLAs are common among services providers that provide external information system services to government agencies;
- Any specific security-related needs to which government agencies wish service providers had a specific capability or security control; and
- Any specific security-related risks to which government agencies wish service providers had a specific capability or security control.

Part 3: Possible provisions for data confidentiality in SLAs. Participants were asked to tell about their perceptions of security-related SLAs, as follows:

- What the possible provisions for data confidentiality are relevant to the Government's data confidentiality requirements; and
- Any specific security-related provisions to which government agencies wish service providers had a specific capability or security control.

6.2.5 Data Collection and Analysis

The Delphi study took several months to complete. The research activities were composed of an adaptive wideband Delphi study and grounded theory analysis. The Delphi approach was used to collect data from participants. Then, the grounded theory approach was used to analyse the Delphi study data. The data collection and analysis consisted of three phases of the grounded Delphi study, as follows and shown in Figure 6.3:

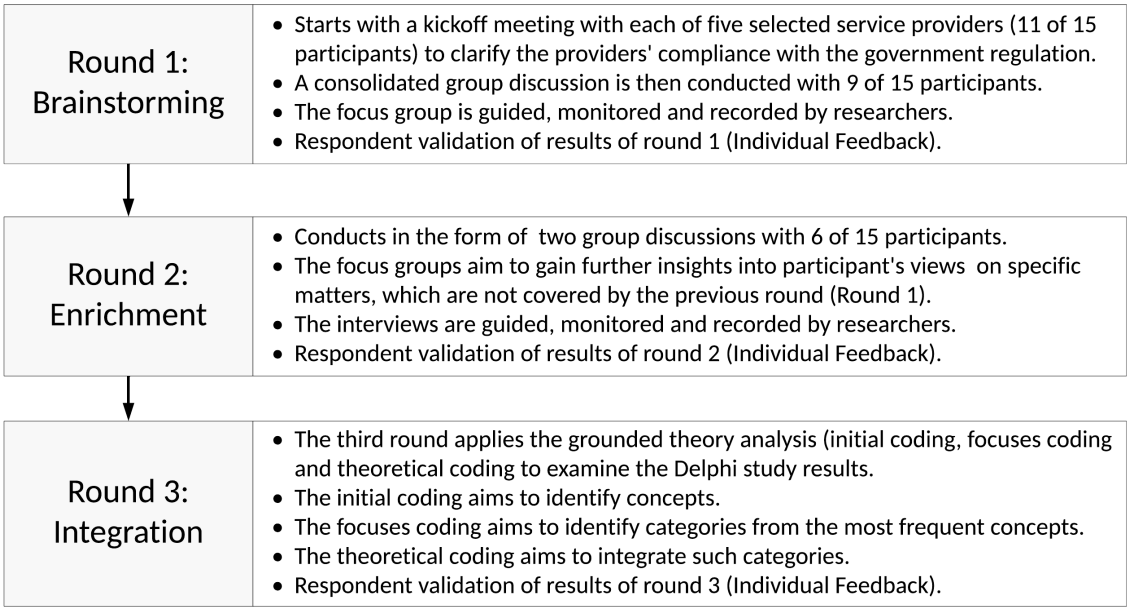


Figure 6.3: Phases of the Grounded Adaptive Delphi Method (GADM)

Brainstorming Phase. The brainstorming session started with a kickoff meeting with each of five selected service providers. One service provider did not take part in the meeting due to duty calls. Each group was intended to clarify the service providers' understanding of their obligations to have agreements on service level and information security. Following this, a consolidated focus group was conducted with representative participants from the five selected service providers. The group discussion aimed to explore a rich understanding of participants' experiences and to generate information on collective views [135]. This phase invited 15 participants who initially agreed to participate in the study. However, only nine participants (n=9) from the five service providers attended the focus group.

Enrichment Phase. This phase conducted an enrichment session using group discussions to elicit detailed information from participants based on the results of the previous phase. This round invited 15 same participants from five selected service providers to participate in the third round. However, only six participants (n=6) from two selected service provider (*SP1* and *SP2*) participated in this phase. The two service providers were the major service providers who were the winner of government tenders in Indonesia, and their service and infrastructures were reported to be compromised according to the secret documents made public by Edward Snowden in 2013 [14].

Integration Phase. The third phase applied the grounded theory analysis (initial coding, focuses coding and theoretical coding) [106–108] to examine the Delphi study data, and to categorise the extracted statements. The initial coding aimed to identify concepts from which the researcher extracted useful sentences or statements. The focuses coding aimed to identify and select categories from the most frequent or significant codes or concepts [108]. Once categories were identified, the theoretical coding aimed to integrate such categories into concepts of provisions for data confidentiality in SLAs. For a validation purpose, these findings were sent to each participant, who was asked for final feedback and corrections if any. The results of round 3 therefore constitute the final results of the GADM study.

6.3 Findings

This section presents the findings from the data collection. In designing and analysing the Delphi study data, the section focuses on several primary research questions, as follows:

1. What are the risk perception of service providers when providing external information system services to government agencies;

2. What are the current provisions of service level agreements provided to government agencies; and

3. What are the possible service provisions for data confidentiality that can be considered for inclusion in service level agreements.

By applying an appropriate qualitative analysis [108], this chapter identifies important codes and categories that emerged from the Delphi study data, and reports the raw number of participants who discussed a specific code to give an approximate indication of its prevalence amongst participants. It is note that some participants failing to mention a particular concept does not necessarily mean that it is irrelevant to such participants.

6.3.1 Key Findings

Before presenting detailed results, this subsection briefly highlights the key findings of this study related to the research questions.

Firstly, participants reported that no specific security requirements were considered as instruments of selecting external service providers that provide cloud-based services, data centre services and network and infrastructure services to government agencies. Another lesson learned from this study is that government agencies do not initially know how to protect government data against unauthorised access, what types of risks to mitigate, what types of data confidentiality requirements that need to be defined, and which controls that need to be employed.

In this case, this study reveals that government agencies heavily rely on the experience of service providers in implementing appropriate security controls to protect sensitive government data against a range of applicable threats and risks. Since government agencies place importance on service availability, a distributed denial of service (DDoS) attack is perceived as the primary security concern. It is clear that such an attack is not concerned with provisions that related to the confidentiality of sensitive government data. However, several participants raised other security concerns related to unauthorised access. The identification of such risks is useful to apply appropriate security controls to protect sensitive data.

Secondly, the findings of this study indicate that the Government's requirements drive the provisions of SLAs offered by service providers. In this investigation, the comments from the participants point out that the Government's requirements only focus on the system availability and performance aspects. Additionally, participants reported that government agencies did not specify specific security capabilities required to protect any future threats

when procuring and using cloud-based services, data centre services and network and infrastructure services from external service providers.

The SLAs implemented by services providers are based on the provision of availability of services, including response time and resolution time. Service providers claim to provide the best-effort services to help ensure the services remain available in case of failure or security incidents by employing security controls and features without the additional cost of security services. However, such claims are not explicitly mentioned in SLAs. In other words, an SLA would be pointless without specifying the security controls expected from service providers.

Thirdly, this study reveals that certifications schemes, such as ISO/IEC *27001*, are paramount in assuring government agencies about the quality of protection provided when handling sensitive government data. In other words, government agencies and services providers rely on the information security management system (ISO/IEC *27001*) to guarantee the security of services. Such certification is a standard security examination designed for government procurement when using external information system services, such as cloud-based services. Although the use of security controls from ISO 27002 is typically mentioned in contracts, it is not sufficient to address the specific threats of unauthorised access that government agencies and service providers are attempting to counter.

6.3.2 Risk Perception

This subsection identifies the risk perception of service providers when providing services to government agencies. Participants reported some security risks in providing external information system services (e.g. cloud-based services) to government agencies. There were similarities amongst participants regarding such risks in the provision of services. For instance, several participants mentioned specific threats concerning *the distributed denial of services (DDoS) attack*. Table 6.2 highlights the perceived risks, as follows:

Table 6.2: Risk Perception

Category	Concept	Focus	No. of Participants (of 15)
Denial of	Identifying DDoS attack	A	4
Access	Identifying traffic anomaly (inbound)	A	1
Collaborator	Identifying misuse by authorised users	C, I, A	1
	Identifying insider threats by employees	C, I, A	3
Exfiltration	Identifying data exfiltration	C	2
	Identifying traffic anomaly (outbound)	C	1
	Identifying key exfiltration	C	1
Insertion	Identifying a malware injection	C, I, A	1
	Identifying a ransomware installation	C, I, A	1
Observation	Identifying interception (traffic)	C	1

6.3.2.1 Unauthorised Denial of Access

Several participants (4 of 15) discussed this type of risk as a central security concern. The perception of such risk allows an adversary to prevent legitimate users from accessing the data or services. Thus, the participants of this study paid much attention to mitigate such risk. Two representative participants reported the following statements:

> "*Our concern as a service provider is related to DDoS attacks because we were victims of the DDoS attacks many times in one month*"—(P11).

The statement above was coded as the concept of identifying a DDoS attack. The concept was categorised as *denial of access*. P1 also noted similar concern, as follows:

> "*For example, while the SWIFT attack hit several banks in the world, we and some other service providers were required to protect against DDoS attacks. Although such attack scenarios did not relate to DDoS attack, in general, if an attack has occurred, the consumers would ask for protection from such an attack.*"—(P1).

6.3.2.2 Collaborator

Participants were concerned with malicious actions by people as the weakest link in the security chain of trust. The perception of such risk allows an adversary through an insider to perform unauthorised use of sensitive data. One participant pointed out that authorised users could perform malicious actions to obtain sensitive data, as follow:

"*We consider the major risk is that authorised users can perform abuse or malicious actions in the organisation*"—(P6).

The statement above was coded as the concept of identifying misuse by authorised users and entities. The concept was categorised as the *collaborator*. P1 also reported similar perception and understanding of the threat model, as follows:

"*if we talk about security considerations, tapping should not be possible in this case, unless done by an insider*"—(P1).

6.3.2.3 Exfiltration

Participants discussed the importance of preventing an unauthorised transfer of data, as the identification of such risk allows an adversary to transmit sensitive data externally. Several participants (2 of 15) indicated the risk of data exfiltration in the following statement:

"*An effort is needed so that data cannot be read and transferred by other people while data is in storage*"—(P1).

The statement above was coded as the concept of identifying misuse by authorised users. The concept was categorised as *exfiltration*. P1 also reported similar perception, as follows:

"*When encrypted, the key management was generated and stored by the customer, not by the provider.*"—(P1).

6.3.2.4 Insertion

Several participants (2 of 15) expressed concern about viruses or malware. Participants reported that the perception of such risk could be inserted into systems. P5 noted the following statement:

"*In case of risks related to malware and viruses, we have anticipated through checking the devices*"—(P5).

The statement above was coded as the concept of identifying a malware injection. The concept was categorised as *insertion*. P1 also reported similar perception, as follows:

> "*if we encrypt the data, even later we will be worried about the data cannot read, even later can be suspected as ransomware*"—(P1).

6.3.2.5 Observation

One participant reported the importance of secure connections in which an adversary could not intercept such communications from the target people or devices, as indicated in the following statement. Such a statement was coded as the concept of identifying interception (traffic) and categories as the *observation* :

> "*If the Internet is used by customers to send sensitive information without using a secure protocol, an attacker can intercept the communication*"—(P1).

In short, this subsection has identified ten concepts of risk perception within five categories that emerged from the Delphi data. The majority of concepts identified were linked to the categories of risk perception identified in Chapter 5, except one category regarding the denial of access, which was not concerned with the confidentiality of government data. In other words, the risk perceptions of participants were interrelated to identifying unauthorised access to sensitive government data.

6.3.3 Current Provisions of Service Level Agreements

This subsection identifies the current provisions of SLAs provided to government agencies that are common among representative service providers. The following table (Table 6.3) highlights several general provisions of SLAs for external information system services where applicable.

6.3.3.1 Availability

Many participants (10 of 15) placed importance on availability with approximately 99.5%. Several participants reported that an availability provision from a security consideration also

Table 6.3: Current Service Provisions of Service Level Agreements

Category	Concept	No. of Participants (of 15)
Availability	Providing system availability (99.5%)	10
	Providing high availability guarantees with additional security solutions	2
Response Time	Providing response time guarantees	6
Resolution Time	Providing response time guarantees	6
Other	Providing jitter levels	1
	Providing downtime insurance	1

addressed the availability of security controls and features to ensure public services keep operating as usual in case of security incidents or events.

> "*If consumers ask for 99.5% availability, we will provide a specific topology, such as the dual-homed gateway to meet such requirements. Further, additional provisions are provided related to the availability of firewalls, intrusion defence systems, intrusion prevention systems and anti-DDoS attacks*"—(P1).

The statement above was coded as the concept of identifying system availability. The concept was categorised as *availability*. Another example, P2 noted the following statement:

> "*For physical security, we have CCTV devices, door access control and visitor access management, while for network security, we have firewall devices, IDS/IPS and load balancer*"—(P2).

6.3.3.2 Response Time

Many participants (6 of 15) reported that response time was one of SLA provisions. Participants pointed out that such provision referred to the total amount of time it takes to respond a request from customers. According to one example of tender documents, as shown in Appendix B, response time was categorised into three classes (less than 30 minutes, within 30 minutes and more than 30 minutes). Participants also reported that the existing SLAs guarantee such provision. For example, P4 reported the following statement.

> "*We will provide the best SLAs. For security needs, we will provide the best-effort services as needed, and ensure the service remains operational. The response, restore and resolve time requirements will be incorporated into the SLA*"—(P4).

6.3.3.3 Resolution Time

Similar to the response time attribute, participants reported that resolution time was also incorporated into the scope of SLAs. Participants noted that such provision referred to the total amount of time it takes to provide a resolution to the request. The total amount of time may differ depending on the categories of services. Participants pointed out that such amount of time for resolution time was expressed in SLA contexts. For example,

> "*The majority of SLA attributes are commonly associated with the availability aspect; other attributes are commonly given related response time and resolution time*"—(P13).

6.3.3.4 Other Provisions

Other provisions typically included in the SLA are downtime, latency, jitter, and packet loss. The metrics of such provisions vary depending on the services provided and the customer needs. For example, P9 noted the following statement:

> "*Most of the services provided is guaranteed by standard SLA criteria. If customers want to include other attributes, such as jitters and downtime, we will provide a customised SLA*"—(P9).

In conclusion, this subsection has identified and described six concepts within four main categories that found from the Delphi study data. It is evident that most of the categories were not novel and well-known, as the objective was to understand the current provisions of SLAs. However, the findings are useful to government agencies and services providers in incorporating data confidentiality requirements into SLA contexts.

6.3.4 Provisions for Data Confidentiality in Service Level Agreements

This subsection examines the Delphi study data to present potential service provisions for data confidentiality which can be incorporated into SLAs. Although participants stated that the provisions related to data confidentiality in SLAs do not yet exist, participants were

asked to mention any security provisions provided to government agencies. The statements made by participants indicated that provisions for data confidentiality were divided into four main categories, namely: 1) technical security provisions; 2) physical security provisions; 3) procedural security provisions; and 4) human security provisions, as shown in Table 6.4.

Table 6.4: Provisions for Data Confidentiality in Service Level Agreements

Category	Concept	No. of Participants (of 15)
Technical Security Provisions	Providing secure connections	5
	Providing authentication and authorisation	5
	Providing access control	4
	Providing encryption	3
	Providing key management	2
	Providing data isolation	2
	Providing malware protection	1
	Providing data breach notification	3
Physical Security Provisions	Providing security cages	1
	Providing access cards	1
	Providing visitor access	1
	Providing CCTV	1
Procedural Security Provisions	Providing vulnerability assessment	1
	Providing penetration testing	1
	Providing compliance with standards	4
	Providing user access matrix	1
Human Security Provisions	Providing security training	4
	Providing personnel security	3

6.3.4.1 Technical Security Provisions

Most commonly, participants mentioned using technical controls or capabilities as security provisions. According to participants, such provisions were given to government agencies but not included in contracts or SLAs. Such provisions constituted minimal or additional services. For example, P2 noted the following statement.

> "*In the context of cloud computing, the required security requirements are mostly related to the connectivity with virtual private networks*"—(P2)

The statement above was coded as the concept of secure connections. The concept was categorised as *technical security provisions*. Another example, P6 reported the following statement which was coded as the concept of encryption levels:

"*For data in motion, we can do encryption, using SSL, IPSec or VPN. For data at rest, we can make use of data encryption and data loss prevention, and for more advanced technologies for cloud customers, we can provide storage encryption or hardware security module*"—(P6)

6.3.4.2 Physical Security Provisions

Participants also mentioned that physical security-related provisions might be included in the SLAs because an authoritative body or an independent third party assessment may audit such provisions. As reflected in Table 6.4, several participants mentioned physical security measures, such as doors, locks, and surveillance tools to deny unauthorised access to facilities and resources. Those concepts were categorised as *physical security provisions*. For example, several participants pointed out some physical security provisions, as follows:

"*We guarantee the availability of CCTV devices, door access and visitor access management*"—(P2).

"*To enter the data centre, there are controls in place to prevent misuse. Also, there is a log book, and the server is caged and locked at a standard facility*"—(P1).

6.3.4.3 Procedural Security Provisions

Several participants (4 of 15) reported the importance of having compliance with security controls, such as ISO/IEC 27002. One participant mentioned vulnerability assessment and penetration testing could serve as security services provided to government agencies. Another participant expressed concerned about the importance of providing user access matrix to controls authorised users to sensitive data. Such concepts were categorised as procedural security provisions. Two participants noted the following statements:

"*Vulnerability assessment and penetration testing services can be provided to customers if needed*"—(P5).

"*We should comply with ISO 27000 series because there already has service delivery, service agreement, third party agreement, assurance, cryptography and so on. It should be enough for us to define confidentiality requirements in SLAs. The standard covers not only technology but also covers People and Process*"—(P6).

6.3.4.4 Human Security Provisions

Several participants (4 of 15) reported the importance of providing security training to customers. Other participants (3 of 15) expressed concerns about personnel security to prevent unauthorised access by authorised users. Such concepts were categorised as human security provisions. Two participants noted the following statements:

"*If we consider security, we not only look at from the technology side, but we must know how the process and procedure. Personnel should be well-educated or know what to do. Once he has access rights, it must be managed properly*"—(P5).

"*We have to protect sensitive data from insider threats*"—(P6).

In short, this subsection has identified and described 18 concepts within four main categories which emerged from the Delphi study data. The four categories of service provisions for confidentiality, namely: 1) technical security provisions; 2) physical security provisions; 3) procedural security provisions; and 4) human security provisions. The findings indicate that participants reveal possible provisions for data confidentiality which can be considered for inclusion in SLA contexts. The preferences for such provisions are evident even though there will be room for improvement to classify such provisions into discrete levels of security assurance.

6.4 Discussion

This section compares the findings of this study with extant literature and details where the findings confirm or contradict the literature, as well as elaborates on the implications of the findings for the Government. The section then makes concrete recommendations for how the findings can be used to motivate government agencies and service providers to incorporate the Government's data confidentiality requirements in SLAs.

6.4.1 Reflection on Related Work

Table 6.5: Potential Service Provision for Data Confidentiality in SLAs

Category	Concept	ISO/IEC 27002	NIST SP 800-53	Common Criteria
Technical Services	Providing secure connections	A.13.1.1	SC-7/8	FDP
	Providing identity management	A.9.2.1	IA.-2/3/4	FIA
	Providing access control	A. 9.1.2	AC-3/6	FMT
	Providing encryption levels	A.10.1.1	SC-13	FCS
	Providing key management	A.10.1.2	SC-12	FCS
	Providing isolation	A. 13.1.3	AC-4/SC-7	FDP
	Providing Malware Protection	A. 12.2.1	AT-2/SI-3	FAU
	Providing data breach notification	A. 16.1.2	IR-6	FAU
Physical Services	Providing security cages	A. 11.1.3	PE-3	None
	Providing access cards	A. 11.1.2	PE-2/3	None
	Providing visitor access	A. 11.1.2	PE-2/3/8	None
	Providing CCTV	A. 11.1.1	PE-3/6	None
Procedural Services	Providing vulnerability assessment	A.12.6.1	RA-5	AVA
	Providing penetration testing	None	CA-8	AVA
	Providing compliance with standard	A. 18.2.2	All XX-1 Controls	AVA
	Providing user access matrix	A.9.2.2	AC-2	FMT
Human Services	Providing security training	A. 7.2.2	AT-2	None
	Providing personnel security	A. 7.1.1	PS-3	None

As discussed in Chapter 2, the existing standards and guidelines, such as ISO/IEC 27002, NIST SP 800-53 and Common Criteria (CC) provide security controls concerning provisions for data confidentiality. The ISO 27002 standard is one of the security standards that widely used by many government agencies. Such a standard contains 114 detailed controls in 14 domains with 35 control objectives. This standard is achieved through a checklist approach of security controls to consider as compliance. Most of the concepts of provisions that emerged from the data are associated with the ISO 27002 controls, as shown in Table 6.5.

Some security controls that are correlated with the findings, namely: A.13.1.1: Network Controls; A. 9.2.1: User registration and de-Registration; A. 9.1.2: Access to Network

and Network Services; A. 10.1.1: Policy on the Use of Cryptographic Controls; A.10.1.2: Key Management; A. 13.1.3: Segregation in Networks; A.16.1.2: Reporting Information Security Events; A.11.1.3: Securing Offices, Rooms and Facilities; A.11.1.2: Physical Entry Controls; A.11.1.1: Physical Security Perimeter; A.12.6.1: Management of Technical Vulnerabilities; A.18.2.2: Compliance with Security Policies and Standards; A.9.2.2: User Access Provisioning; A.7.2.2: Information Security Awareness, Education, and Training; and A.7.1.1: Screening. The existence of such a certification aims to provide enough evidence that the product and software hold some security properties and behaves as expected [50, 87].

Many certification schemes, such as ISO/IEC 27001 have become prominent in outsourcing and service provisioning environments, especially for the context of the Government of Indonesia. The security controls from the ISO/IEC 27002 standard is typically incorporated into contractual agreements. However such agreements do not specify what security controls or levels of security are guaranteed. This thesis focuses on an understanding of how to incorporate such provisions for data confidentiality into SLA contexts. Incorporating such security controls into contracts or SLAs constitute a security-related SLAs. However, the level of assurance for each security control expressed in SLAs needs to be defined according to the data classification and threat model.

Likewise, the NIST also provides a foundation of security controls for provisioning data confidentiality. The standard provides a catalogue of security and privacy controls, which are intended for the federal agencies and those conducting business with the US government. The provisions for data confidentiality that emerged from the Delphi study data are linked to the NIST controls, as shown in Table 6.5. Some security controls are in line with the findings, namely: SC-7: Boundary Protection; SC-8: Transmission Confidentiality and Integrity; IA-2: Identification and Authentication; IA-3: Device Identification and Authentication; IA-4: Identifier Management; AC-3: Access Enforcement; AC-6: Least Privilege; SC-13: Cryptographic Protection; SC-12: Cryptographic Key Establishment and Management; AC-4: Information Flow Enforcement; IR-6: Incident Reporting; PE-3: Physical Access Control; PE-2: Physical Access Authorisations; PE-6: Monitoring Physical Access; PE-8: Visitor Access Records; RA-5: Vulnerability Scanning; CA-8: Penetration Testing; AC-2: Account Management; AT-2: Security Awareness Training; and PS-3: Personnel Screening.

Such a catalogue of security controls is necessary for expressing the Government's data confidentiality requirements in SLAs. Interestingly, according to Duncan and Whittington, compliance with security standards, such ISO/IEC 27002, NIST and Cloud Security Alliance [23] is more likely to ensure compliance with a particular security standard, rather than achieve a significant level of security. Anderson [19] also supports this argument. However, such controls are needed to be formulated and classified to define specified security assurance levels for each security control expressed in SLAs.

Similarly, CC is also often used as the basis for government-driven certification schemes. This standard aims to evaluate and certify products and systems in a predefined set of categories, each with different security requirements. The provisions for data confidentiality that emerged from the data are also associated with the security functional and assurance components of common criteria, as shown in Table 6.5. Such criteria for IT security include FDP: User Data Protection; FIA: Identification and Authentication; FMT: Security Management; FCS: Cryptographic Support; FAU: Security Audit; and AVA: Assurance Vulnerability Analysis. However, some of the concepts that emerged from the data are not covered by CC because of such provisions related to physical and human provisions.

This condition is in line with CC, which is often used as the basis for security evaluation for information technology products or systems, especially those focused on high-assurance systems [15, 18]. The CC certification scheme is known to be slow-moving, which is problematic and unlikely to be appropriate for services, and causes substantial costs of security services to the suppliers or service providers [15]. The CC scheme has been criticised as a highly bureaucratic system rather than providing genuine security enhancement [19] because it carries the cost of security assurance for the certification scheme. Furthermore, according to Anisetti et al. [24], existing certification schemes, such as CC and ISO/IEC 27001 are not well-suited to the service scenario, such as cloud-based services. Bohme [15] and Anderson [19] demonstrate that such schemes do not ensure better security and cannot contribute to addressing emerging threats and vulnerabilities.

In short, the comments from the participants indicate that service providers rely on certification schemes to guarantee the security of services. Such certifications are typically aimed at compliance with a particular security standard, rather than achieve a specified level

of security. In essence, certification schemes for higher-grade work are mostly focused on products. Therefore, it is essential to state that the currently available certification schemes are unlikely to be appropriate for securing external information system services.

6.4.2 Main Outcome

From service providers' perspectives, this chapter considers the following outcome to be the most important ones from the findings:

- The significant finding from this study is that government agencies place essential requirements on service availability, including response time and resolution time and they do not demand security requirements, such as data confidentiality. This is because the perception of SLAs, from a government perspective, is solely about the service availability and performance aspects. Therefore, based on the findings from the Delphi study data, the formulation of security requirements regarding data confidentiality can be incorporated into SLA contexts.

- The statements from the participants indicate that service providers find it difficult to address data confidentiality in SLAs. Therefore, government agencies make use of the provision of service availability to demand additional means of confirming the security of services supplied by service providers. For example, some government agencies require the availability of security controls and features, such as the availability of firewalls, access controls, visitor access management, intrusion detection systems, intrusion prevention systems, and closed-circuit television (CCTV).

- Certifications schemes, such as ISO/IEC *27001*, are paramount for meeting government security compliance regulations. It is apparent that the information security management system (ISO *27001*) certification is often the only available way to demonstrate compliance with the Government's regulations to provide a degree of security assurance. Therefore, service providers are required to hold the ISO *27001* certification when providing such external services to government agencies, particularly for the Government auctions at the value above *IDR 5 billion (GBP 320 thousand)*, as shown in Table 6.7.

6.4.3 Recommendations

This study distils from the findings the following recommendations for where government agencies and service providers in Indonesia can focus on its efforts.

- **Develop a practical approach for adequately expressing security aspects in SLAs**. Government agencies and services providers have perceived lack of security agreements in standards. Certification schemes have been employed in service provision and outsourcing environment. However, such certifications are mostly unsuitable in the context of service provisioning and do not ensure better security. Therefore, both parties should elaborate on the application of SLAs as trust-enhancing instruments. In other words, it is necessary to incorporate adequate assurance levels for each security control related to data confidentiality provisions into SLAs. Such an approach aims to establish an adequate level of trust between both parties and to reach and guarantee a discrete level of assurance that can satisfy the Government's data confidentiality requirements against unauthorised access.

- **Strengthen the roles of SLAs for data confidentiality in business relationships**. Many services providers offer SLAs in supporting various service dimensions, such as availability, response time and resolution time to government agencies. To date, the roles of SLAs are limited to defining guarantees and regulations regarding service availability and quality of services. With the focus on protecting sensitive government data when using such external services, it makes sense to adapt SLA-based discrete levels of assurance as trust-enhancing instruments. The SLAs implemented by service providers are based on provisions that can be measured, such as 99.5% availability. Such provisions can be predicted based on the previous measurements and is well-understood by government agencies and service providers. However, the concept of SLAs for security provisions is relatively new to government agencies and service providers. Therefore, it is useful to examine how SLA-based discrete levels of assurance can be used as an assurance evidence to establish trust between government agencies and service providers and to ensure appropriate security levels are expressed in SLA contexts and consistently maintained and updated.

6.5 Chapter Summary

This study has examined the current provisions of 'real-world' SLAs offered to Indonesian government agencies when providing external information system services (e.g. cloud-based services, data centre services and infrastructures). The study has also identified potential service provisions for data confidentiality in SLAs that have emerged from the Delphi study data. The findings show that the SLA implemented by services providers are based on provisions that can be measured, such as availability, response time and resolution time. Although service providers find it difficult to address the Government's data confidentiality requirements in SLA contexts, several data confidentiality capabilities have been identified by participants as possible provisions for data confidentiality in SLAs. Such provisions are in-line and consistent with security control catalogues from ISO 27002 and NIST SP800-53.

As the findings emerged from the statements of participants, it is essential to compare such findings (concepts and categories) with related work. The findings motivate to incorporate adequate assurance levels for each control related to data confidentiality into SLA contexts. The evidence from this chapter suggests that there is a need for an approach that can potentially adequately express the Government's data confidentiality requirements in SLAs. The findings also highlight the need to enhance the roles of SLAs for data confidentiality in service provider relationships when using external information system services.

Therefore, further research is required to develop the concept of assurance and trustworthiness through SLAs when the Government procures and uses external information system services (e.g. cloud-based services) from external services providers. The following chapter presents principles as foundations for a TDSLA capability framework as a means of incorporating the Indonesian Government's data confidentiality requirements into the formulation of SLA-based discrete levels of security assurance.

Table 6.6: Procurement on External Information System Services

ID	Website	Total	DC	Cloud	Colocation	Internet	Network
EP01	*lpse.big.go.id*	608	20	5	0	2	0
EP02	*202.137.7.70*	134	0	0	0	0	3
EP03	*lpse.bakamla.go.id*	7	0	0	0	0	0
EP04	*lpse.bkkbn.go.id*	420	1	0	0	0	3
EP05	*lpse.bkpm.go.id*	324	2	0	3	0	6
EP06	*lpse.bmkg.go.id*	913	0	1	0	12	4
EP07	*lpse.bnn.go.id*	269	1	1	0	0	3
EP08	*lpse.bnpb.go.id*	380	4	0	1	0	5
EP09	*lpse.bnpt.go.id*	60	0	0	0	0	0
EP10	*lpse.bnpt2tki.go.id*	123	6	0	2	1	1
EP11	*lpse.bnpp.go.id*	53	0	0	0	0	0
EP12	*lpse.pom.go.id*	836	3	0	0	3	2
EP13	*lpse.bppt.go.id*	39	0	0	0	0	0
EP14	*lpse.bpn.go.id*	1011	5	0	0	6	0
EP15	*lpse.bps.go.id*	251	5	0	0	4	0
EP16	*lpse.basarnas.go.id*	684	1	0	0	0	2
EP17	*lpse.dpd.go.id*	44	0	0	0	1	1
EP18	*lpse.dpr.go.id*	247	0	0	0	4	0
EP19	*lpse.kejaksaan.go.id*	217	0	0	0	2	0
EP20	*lpse.kemenag.go.id*	5798	4	0	0	2	10
EP21	*lpse.kemendagri.go.id*	1209	19	0	0	7	16
EP22	*EP.esdm.go.id*	2975	6	3	1	6	5
EP23	*lpse.kemenkumham.go.id*	3771	3	0	2	2	10
EP24	*lpse.dephut.go.id*	2232	0	0	0	1	2
EP25	*lpse.kkp.go.id*	2964	1	0	0	0	0
EP26	*lpse.depkes.go.id*	7062	12	0	0	0	9
EP27	*lpse.kemenkeu.go.id*	10226	80	3	2	84	21
EP28	*lpse.kominfo.go.id*	275	1	1	1	1	1
EP29	*lpse.polkam.go.id*	35	2	0	0	0	0
EP30	*lpse.depkop.go.id*	607	2	0	0	2	0
EP31	*lpse.kemlu.go.id*	156	3	3	0	3	0
EP32	*lpse.ristekdikti.go.id*	274	2	0	0	2	2
EP33	*lpse.kemenpar.go.id*	1567	1	0	0	2	1
EP34	*lpse.pu.go.id*	10935	1	0	4	1	0
EP35	*lpse.kemendesa.go.id*	1436	1	0	0	0	1
EP36	*lpse.kemenpora.go.id*	164	0	0	0	0	0
EP37	*lpse.menpan.go.id*	55	0	0	0	1	1
EP38	*lpse.kemendikbud.go.id*	3405	33	5	0	9	8
EP39	*lpse.kemendag.go.id*	488	6	0	0	6	1
EP40	*lpse.dephub.go.id*	20632	7	1	0	6	17
EP41	*lpse.kemenperin.go.id*	2031	4	0	0	9	11
EP42	*lpse.kemhan.go.id*	159	0	0	0	0	0
EP43	*lpse.pertanian.go.id*	1744	4	0	0	5	0
EP44	*lpse.kemsos.go.id*	880	4	0	0	3	5
EP45	*lpse.depnakertrans.go.id*	-	-	-	-	-	-
EP46	*lpse.polri.go.id*	2866	3	0	0	0	13
EP47	*lpse.lipi.go.id*	613	2	3	0	8	3
EP48	*lpse.lkpp.go.id*	1679	15	2	1	23	50
EP49	*lpse.lemhannas.go.id*	144	0	0	0	0	4
EP50	*lpse.lapan.go.id*	141	1	0	0	6	0
EP51	*lpse.lemsaneg.go.id*	226	4	2	0	1	13
EP52	*lpse.mahkamahagung.go.id*	1462	3	0	0	1	1
EP53	*lpse.mahkamahkonstitusi.go.id*	88	0	1	0	0	1
EP54	*lpse.mpr.go.id*	62	0	0	0	1	0
EP55	*lpse.dkn.go.id*	11	1	0	0	0	1
EP56	*lpse-mabestni.mil.id*	9	0	0	0	0	0
EP57	*lpse.tniad.mil.id*	788	0	0	0	0	0
EP58	*lpse.tnial.mil.id*	118	0	0	0	0	0
EP59	*180.243.87.93*	46	0	0	0	0	0

Table 6.7: Procurement at the values above IDR5 billion (£320 thousand)

Acquirer	Year	Service Procured	Security	Cost (IDR-Billions)	% Saving	SP
Ministry of Finance	2010	Data Communication Network	NM	5.092.910.240,00	46.16%	SP 2
	2010	Data Communication Network	NM	9.516.314.500,00	0.49%	SP 1
	2011	Data Communication Network	NM	11.724.325.360,00	1.64%	SP 1
	2011	Data Communication Network	NM	10.768.748.131,00	3.26%	SP 1
	2013	Data Communication Network	ISO 27001	12.755.820.000,00	0.27%	SP 1
	2013	Data Communication Network	ISO 27001	19.277.843.200,00	1%	SP 1
	2015	Data Communication Network	NM	21.392.624.880,00	1.77%	SP 1
	2015	Data Communication Network	NM	12.455.537.600,00	3.32%	SP 1
Attorney General's Office	2013	Internet & VPN	ISO 27001	28.537.590.950,00	0.75%	SP1
	2014	Internet & VPN	ISO 27001	28.001.118.915,00	0.32%	SP 1
	2015	Internet, VOIP, Video	NM	28.983.024.235,00	0.38%	SP 1
	2016	Internet, VOIP, Video	ISO 27001	29,034,192,000.00	1.16%	SP 1
Ministry of Social Affairs	2014	Internet Connections	ISO 27001	26.219.391.000,00	14.49%	SP1
	2015	Internet Connection	ISO 27001	37.273.318.500,00	0.59%	SP 1
	2015	Data Communication Network	ISO 27001	7.030.964.600,00	1.71%	SP 1
	2016	Data Communication Network	ISO 27001	13.298.053.450,00	2.89%	SP 1
	2016	Data Communication Network	NM	46.454.858.726,00	3.85%	SP 1
National Police	2014	Telecommunication Networks	NM	36.366.423.390,00	8.99%	SP 1
	2015	Telecommunication Networks	ISO 27001	36.565.075.169,00	7.69%	SP 1
	2016	Communication Satellite	NS	5.979.996.000,00	0.11%	SP 8
	2016	Telecommunication Networks	NS	42.257.904.216,00	1.31%	SP 1
Ministry of Health	2012	Telecommunication Networks	NM	23.256.313.859,00	0.65%	SP 1
	2013	Internet and VPN	NM	34.810.666.000,00	0.55%	SP 1
	2014	Information System Network	ISO 27001	37.860.544.920,00	0.50%	SP 1
	2015	Information System Network	NM	36.983.364.000,00	0.37%	SP 1
	2016	Information System Network	NM	12.643.164.600,00	0.01%	SP 1
	2016	Backup Data Centre	NM	9.529.093.200,00	0.01%	SP 1
Ministry of Justice and Human	2013	Leased Network for Immigration	ISO 27001	23,499,713,930.00	1.88%	SP 1
	2014	Leased Network for Immigration	ISO 27001	43.997.466.480,00	9.99%	SP 1
	2015	Leased Network for Immigration	NM	63.783.578.760,00	2.76%	SP 1
	2015	Network Interconnection	NM	7.886.757.340,00	20.30%	SP 1
	2016	Leased Network for Immigration	ISO 27001	45.539.350.560,00	21.36%	SP 1
Ministry of Home Affairs	2012	Data Communication Network	NM	33.681.760.000,00	0%	SP 2
	2013	Data Communication Network	NM	295.017.670.000,00	5%	SP 2
	2014	Data Communication Network	NM	256.461.282.000,00	12.75%	SP 2
	2015	Data Communication Network	NM	253.639.259.630,00	12.77%	SP 2
Ministry of Religious Affairs	2013	Communication Network	NM	12.862.522.332,00	2.77%	SP 1
	2015	Communication Network	NM	13.713.311.150,00	1.74%	SP 1
	2016	Communication Network	NM	14.183.133.712,00	0.25%	SP 1
National Land Agency	2011	Bandwidth on IP VPN and Internet	NM	20.788.489.920,00	1.75%	SP 1
	2012	Bandwidth on IP VPN and Internet	NM	18.477.619.820,00	0.85%	SP 1
	2013	Bandwidth on IP VPN and Internet	ISO 27001	32.454.309.360,00	3.23%	SP 1
	2014	Bandwidth on IP VPN and Internet	ISO 27001	34.478.653.000,00	0.74%	SP 1
	2015	Bandwidth on IP VPN and Internet	ISO 27001	34.963.749.370,00	0.10%	SP 1
	2016	Bandwidth on IP VPN and Internet	ISO 27001	29.989.386.900,00	0.02%	SP 1
Financial Services Authority	2013	Internet and Intranet Services	NM	9.042.426.800,00	5.46%	SP 1
	2015	Data Centre Co-location	NM	31.349.451.375,00	40%	SP 7
	2015	Data Centre Co-location	NM	24.500.025.000,00	51.52%	SP 1
Ministry of Transportation	2016	Data Centre	NM	7.870.396.982,00	3.36%	SP 1
	2016	Data Centre	NM	16.276.344.898,00	0.49%	SP 1
Capital Investment Board	2015	Communication Networks	NM	5.776.563.870,00	4.84%	SP 1
	2015	Bandwidth Networks and Co-location	NM	5.888.493.600,00	1.10%	SP 1
National Library	2015	VPN-IP MPLS and Internet	NM	5.328.016.666,00	3.13%	SP 6
Ministry of Education	2013	VPN Networks	NM	6.119.278.000,00	2.09%	SP 1
Institute of Sciences	2015	Internet and Cloud Services	NM	5.099.999.000,00	1.02%	SP 1
Ministry of Public Work	2016	Internet Bandwidth	ISO 27001	9.528.133.560,00	0.23%	SP 1
Narcotics Agency	2016	Communication Network	ISO 27001	5.808.128.040,00	3.20%	SP 1

7
Framework

> *Everything should be made as simple as possible, but not any simpler.*
>
> Albert Einstein,

Chapter 7 draws on refereed articles described in the following publications:

- Y. Nugraha and A. Martin. Trustworthy Service Level Agreements: An Approach for Protecting Government Data Secrecy. Work in Progress. In 10th Layered Assurance Workshop, Annual Computer Security Applications Conference (ACSAC), 2016.
- Y. Nugraha and A. Martin. Towards the Classification of Confidentiality Capabilities in Trustworthy Service Level Agreements. In Proceedings 5th International Conference on Cloud Engineering (IC2E 2017), pp. 304-310, IEEE, 2017.
- Y. Nugraha and A. Martin. Developing Principles for a Trustworthy Data Security Level Agreement Capability Framework: An Indonesian Government Case Study. This manuscript is in the process of submission to a journal publication.

Contents

7.1 Introduction

Many government agencies rely on a wide variety of assurance schemes to build trust with external service providers that support the delivery of public services. External service providers that process, transmit and store sensitive government data are required to adhere to a duty of confidentiality according to data classification and risk level. The issue of data confidentiality and its inclusion in compliance and audit requirements for service providers seeking security certifications has received considerable attention in this thesis (e.g. ISO/IEC *27000 series* and CC).

As described in Chapter 4, specific government security needs have been proposed to address security within supplier agreements, such as non-disclosure agreements (NDAs), trustworthy system certifications, and information security agreements. An NDA is necessary to begin sharing sensitive information among contracting parties. While certification schemes have tended to focus on products and systems [18], many certification schemes have become essential for government procurement to ensure the security of services.

However, both NDAs and certification schemes are not well suited to the service scenario, as they do not fit into dynamic environments [24], and are not sufficient to address emerging threats and vulnerabilities in a dynamic threat environment [13, 15]. Further, the information security agreement is solely for the purpose mutual trust and understanding of the restricted use of the confidential material, knowledge, or information provided between parties, while the research and development into security clauses in contracts and SLAs is still ongoing.

Debate continues about a tailored and appropriate assurance approach in service provisioning. The reason is that the objective of certification schemes is to help ensure compliance with a security standard rather than achieve a meaningful level of security [19,23]. Therefore, this chapter aims to develop the concept of system assurance and trustworthiness when using external information system services, such as cloud-based services. The application of assurance-based SLAs is essential when using such external services. However, the provision of SLAs only pays attention to the performance and system availability aspects without considering data confidentiality when processing, transmitting or storing sensitive government data [33, 34]. Although extensive research has been carried out on the formu-

lation of security-related SLAs [28–35, 167], there appears to be insufficient coverage of incorporating the Government's data confidentiality requirements into SLAs when using external information system services.

Due to the lack of assurance on the security of information system services in previous studies, the work on the Indonesian Government's data confidentiality requirements provides guidance in developing foundations from the empirical qualitative data derived from the Delphi study data. This chapter presents principles as foundations for a TDSLA capability framework through a qualitative analysis of the two empirical studies (Chapter 5 and Chapter 6), each conducted with different participant groups.

Firstly, an investigation was conducted by asking 35 government participants via group discussions and individual sessions [162]. Secondly, a longitudinal study was carried out using a dataset on government procurement of 59 e-procurement services across 80 government agencies to identify major service providers that provided Internet services, cloud-based services and data centre services to Indonesian government agencies from 2010-2016. Based on the longitudinal study results, five selected service providers were invited, including 15 participants to participate in this study [13]. Finally, a qualitative analysis based on the grounded theory approach was conducted to examine findings from the two empirical studies to identify concepts, categories and principles. The results led to the development of foundations for building a TDSLA capability framework.

This chapter, therefore, provides a significant opportunity to advance the understanding of incorporating the Government's data confidentiality requirements into SLAs. The main contributions of this chapter are as follows: 1) developing principles as foundations for a TDSLA capability framework; 2) describing discrete levels of security assurance that can be incorporated into SLAs; and 3) validating the framework with real-world cases, and through participants' feedback.

The remainder of this chapter is structured as follows. Section 7.2 presents the methodology used to define the principles and framework. Section 7.3 presents principles as foundations for a TDSLA capability framework. Section 7.4 validates the principles and framework using participants' feedback, and two real-world cases from AWS G-Cloud and AWS-FedRAMP. Section 7.5 summarises the chapter.

7.2 Method

This chapter proposes principles as foundations for a TDSLA capability framework between government agencies and service providers, using the work on the Indonesian Government's data confidentiality requirements. Due to the lack of previous studies on the concept of assurance in service provisioning, a qualitative analysis based on grounded theory approach was conducted to develop principles and framework from the data derived from two empirical studies in Chapter 5 and Chapter 6. Each empirical study was conducted in different settings and participant groups. The grounded theory approach is a well-established research methodology by which a proposed framework can be developed through a process of data collection activities, coding and categorisation. This is followed by several comparative and theoretical analyses of findings [106–108, 110, 111, 168], as shown in Figure 7.1

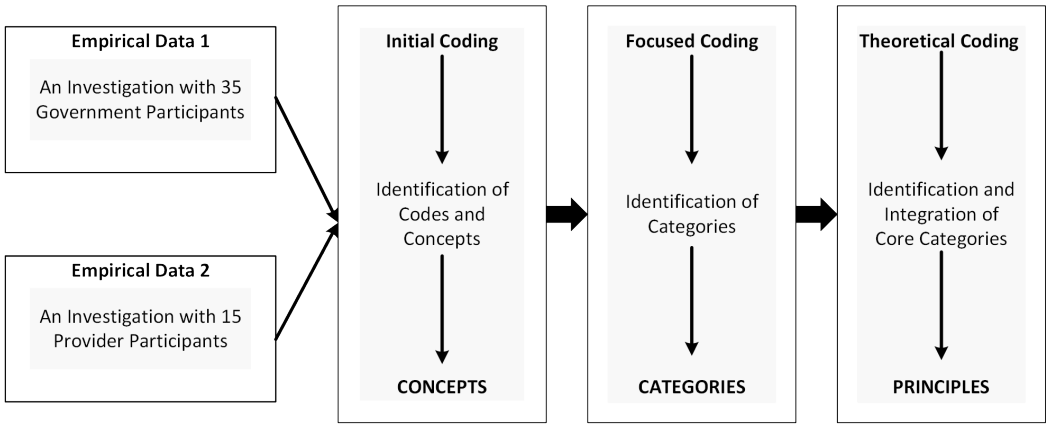


Figure 7.1: The Research Method - A Grounded Theory Approach

7.2.1 Data Sample and Data Collection

In Chapters 5 and 6, two empirical studies were conducted [13, 162] with a total of 50 participants, to explore opinions on how to incorporate the Government's data confidentiality requirements into SLA contexts. Firstly, a set of data collection activities were conducted with 35 government participants via focus group and individual sessions within the scope of the Delphi data collection rounds [162]. Secondly, 15 participants were invited from the five selected service providers that provide information system services to government agencies to participate in the process of the Delphi data collection [13]. Each group discussion

took about 60 to 120 minutes. The individual session took between 20-120 minutes. The group discussion and individual sessions were recorded in audio format and transcribed by a professional transcription service. Original transcripts were not translated into English to keep the original meaning of the text and expression.

7.2.2 Data Analysis

The two sets of empirical data derived from Chapters 5 and 6 were examined using a grounded theory analysis. Validation for Chapter 5 and 6 was carried out through three rounds of the GADM study in which the results of each round were sent to each participant, who was asked for feedback and corrections if any. The results of round 3 for Chapter 5 and 6 therefore constitute the validated data used in this chapter. Furthermore, the procedure for coding used in the grounded theory analysis in this thesis was conducted in three steps: 1) initial coding; 2) focused coding; and 3) theoretical coding [108]. This procedure enables the researcher to use raw data to develop a useful understanding that is summarised in a set of principles, as shown in Figure.7.2.

After organising the data, an initial coding of the transcribed dataset was conducted to identify concepts. The main aim of the initial coding was to discover the principal idea highlighted in each sentence or paragraph. Focused coding was then conducted to identify and select categories from the most consistent or significant codes and using them to categorise specific codes. In the final step, theoretical coding was performed to specify the relationships between core categories to incorporate them into a cohesive framework. All the emerged codes, concepts, categories were compiled to derive principles.

The Oxford Dictionary defines a principle as '*a fundamental truth or proposition that serves as the foundation for a system of belief or behaviour or for a chain of reasoning*'. In this chapter, such a principle contains two or more main categories that are connected using linking words to form a meaningful statement [168]. From this, a framework can be defined as a coherent group of principles. In other words, such principles are the building blocks of developing a TDSLA capability framework. Figure 7.2 shows the complete list of concepts and categories that emerged from the grounded theory approach.

For the latter step, to validate the grounded theory of Chapter 7, an iterative process of definition and validation of principles and framework were conducted by using the participants' feedback. Further, a minimum agreement of 70% from the participants is necessary to be reached to support validation of the principles and framework [110]. Hence, this chapter confirms the correctness and practicability of the principles and framework.

7.3 Framework

This chapter aims to develop principles as foundations for a TDSLA capability framework from work on the Indonesian Government's data confidentiality requirements. The framework presented in Figure 7.2 consists of several categories, depicted in five main categories as proposed principles, as follows:

1. Classifying Government Data;
2. Identifying Data Confidentiality Risks;
3. Defining SLA Data Confidentiality Requirements;
4. Provisioning Data Confidentiality Capabilities; and
5. Formulating Discrete Security Assurance Levels.

Figure 7.2 shows that each box is used to represent a core or main category, which can serve as a principle. Each main category consists of an identified set of subcategories. This section begins from the perspective of what to protect in order to explain the main categories of the framework and their relationships.

Classifying government data is defined so that perceived data confidentiality risks can be managed through data classification. Identifying data confidentiality risks can then define government SLA data confidentiality requirements. Demonstrating the required data confidentiality capabilities in response to government SLA data confidentiality requirements is defined as the activity of demonstrating compliance with the Government's data confidentiality requirements.

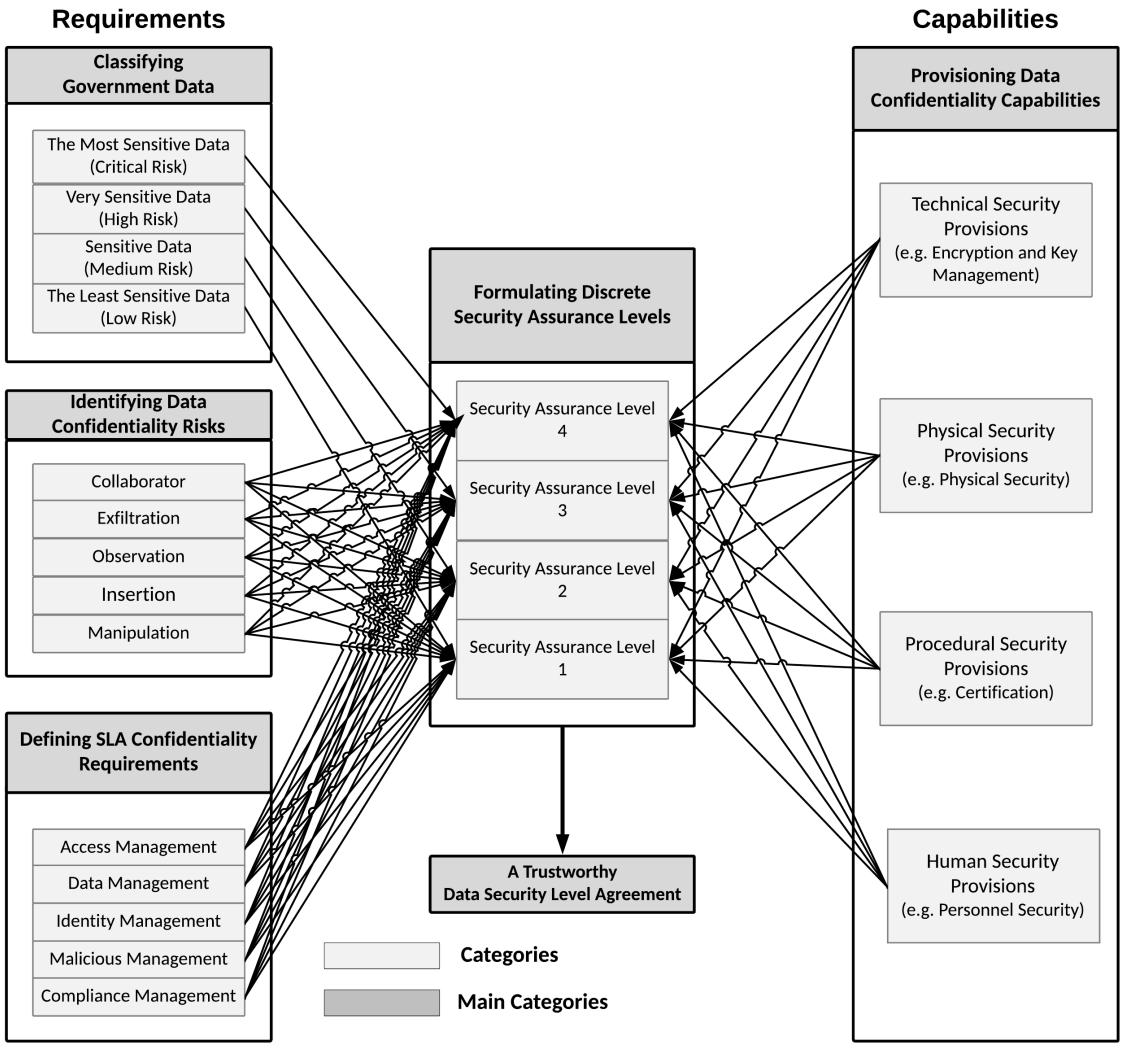


Figure 7.2: TDSLA Capability Framework

Moreover, formulating discrete security assurance levels is determined relative to the interplay of data classification levels, data confidentiality risks, SLA data confidentiality requirements and data confidentiality capabilities. Finally, selecting an appropriate level of security assurance can be incorporated into an SLA.

In the following subsection, principles are formulated from the Delphi study data and defined using the main categories and its associations. Each section begins with a box which enables the source from each principle can be tracked through the analysis which was used in this thesis. The core categories are derived from interpretations of insights from participants. All of such principles are novel and direct insights from this study.

7.3.1 Classifying Government Data

Grounded Theory Analysis Traceability
The theme of this subsection is linked to the following:

- Target of Protection: Information Asset (Sub-subsection 5.3.1.2)

Classifying government data was defined as a process in which government agencies can define an appropriate level of protection needed for a particular information asset. Examples of such information include citizen data, medical records, financial information, and intelligence and military data. Participants agreed that current regulations that classified government data were consistent with their understanding.

However, it is essential to acknowledge various types of data handling and management constraints over the data (e.g. data protection, national security, and health regulations). Therefore, the process of classifying data should incorporate data that is critical to national security, personal data, sensitive business data and publicly available data. In other words, government data at any level of classification should receive consistent levels of protection across the Government and business sectors. This degree of consistency is essential to establish trust between government agencies and service providers.

Four levels of classifications emerged from the findings, namely: 1) the least-sensitive data (low-risk); 2) sensitive data (moderate-risk); 3) very sensitive data (high-risk); and 4) the most sensitive data (critical-risk), as shown in Table 7.1. Such terminologies of data classification can avoid ambiguity in determining an appropriate level of protection against applicable threats. It is note that a specified level of security assurance required for each type of government data was derived from interpretations of insights from participants.

Further, participants reported that data classification and risk assessment are paramount to indicate how government agencies specify a level of security assurance for external services (e.g. cloud-based services) that process, store or transmit government data. In other words, data classification is the principal means of indicating the sensitivity and risk of an information asset and the security requirements for each data classification level. In doing so, it helps to ensure data security, compliance and risk management. Therefore, classifying

Table 7.1: Classifying Government Data

Data Classification	Example	SAL1	SAL2	SAL3	SAL4
The Least-Sensitive	Government Budget	V			
(Low Risk)	Regulations	V			
Sensitive	Health or Medical records		V	V	
(Moderate Risk)	Financial Information		V	V	
	Citizen Data		V	V	
	Personal Data and privacy		V	V	
	Law Enforcement Data		V	V	
	Tax information		V	V	
	National Identity		V	V	
	Email Communications		V	V	
	Natural and energy resource data		V	V	
Very Sensitive	National Economic Interests			V	V
(High Risk)	Confidential Diplomatic Communications			V	V
	Intelligence Data			V	V
	Military and Defence data			V	V
The Most Sensitive	Intelligence Data			V	V
(Critical Risk)	Military and Defence data			V	V

The checklist **(V)** for each SAL (Security Assurance Level) was derived from interpretations of insights from participants. The amount of data that is processed, transmitted and stored affects the level of security assurance.

government data is necessary for formulating a consistent way of protecting government data, as shown in the following quotes from two representative participants.

> "*Classifying data is necessary to define in the first place. Also, we need to understand whom the information owner allowed access*"—(P5-SP).
>
> "*Each ministry should classify its data as public, regulated, restricted, secret and top secret. However, the classification of confidential data in the Ministry A may be different classification with the Ministry B*"—(P19-GOV).

While Article 17 of the Indonesian Law on Public Information Transparency number 14 of 2008 and the Regulation Number 17 of 2011 concerning Government Security Classifications and Archives cover levels of government data classification, participants reported that there was a need for the Government to formulate and classify data confidentiality requirements for each data classification and risk level.

The Law Number 14 of 2008 defines public sector data into three categories of data classification: 1) public; restricted; and secret. Additionally, the Regulation Number 17 of 2011 outlines government security classifications into four levels: 1) public; 2) restricted;

3) secret; and 4) top secret. However, both law and regulation do not define an appropriate level of protection for each data classification. For example, each category should include information about security requirements with rules for processing, transmitting, and storing sensitive data.

Based on the Delphi study data, empirical evidence of the linkage between classifying government data and formulating discrete security assurance levels is limited. Therefore, there is a need to define the linkages between data classification levels and discrete levels of security assurance which can be incorporated into the formulation of SLAs. The findings of this study provide further support for the following principle.

Principle 1

Classifying Government Data *is linked to the process of* ***Formulating Discrete Security Assurance Levels*** *in which an appropriate protection level can be incorporated into a service level agreement.*

7.3.2 Identifying Data Confidentiality Risks

Grounded Theory Analysis Traceability
The theme of this subsection is linked to the following:

- Risk Perception: From A Government Perspective (Subsection 5.3.2)
- Risk Perception: From A Service Provider Perspective (Subsection 6.3.2)

Identifying data confidentiality risks were defined in the grounded theory analysis as a process in which government agencies perceive confidentiality threats to sensitive government data against unauthorised access. Participants reported that three threats actors determined a risk perception: 1) caused by a local adversary (e.g. a customer); 2) caused by a service provider (e.g. a global cloud provider); and 3) caused by a global adversary (e.g. a powerful nation-state). Overall, the statements from participants indicated that identifying data confidentiality risks was associated with the categories of collaborator, exfiltration, observation, insertion and manipulation, as shown in Table 7.2.

Table 7.2: Identifying Data Confidentiality Risks

Data Confidentiality Risk	Example	SAL1	SAL2	SAL3	SAL4
Collaborator	Insider threats by contractors	V	V	V	
	Insider threats by employees	V	V	V	V
	Insider threats by service providers	V	V	V	
	Insider threats by government partners	V	V	V	
Exfiltration	Outbound traffic	V	V	V	V
	Content exfiltration by a service provider	V	V	V	V
	Data exfiltration by connected devices		V	V	
	Key exfiltration by a service provider	V	V	V	
	Data exfiltration by malware	V	V	V	
Observation	Metadata collection by foreign agencies	V	V	V	
	Discovery by foreign governments	V	V	V	
	Interception (content/traffic)	V	V	V	
Insertion	A ransomware installation	V	V	V	V
	A malware injection	V	V	V	V
Manipulation	Phishing attacks	V	V	V	V
	Social engineering attacks	V	V	V	V
	Impersonation attacks	V	V	V	V

The checklist **(V)** for each SAL (Security Assurance Level) was derived from interpretations of insights from participants. Each level is possible to have the same threat model with a different sophistication of the threat environment.

For example, participants discussed the possibility of content or key exfiltration by services providers to obtain sensitive government data. Additionally, participants paid much attention to mitigating data exfiltration and outbound traffic, as shown in the following quotes from two representative participants.

> "*Regarding key management, our customer can hold the encryption keys, even though the encryption process has been created on the provider side*"—(P1-SP).
> "*Security threats and attacks can come from inside government networks. For example, our observation discovered botnets keep sending out the data from the government networks*"—(P13-GOV).

Participants from both the Government and service providers were asked to indicate whether it is possible to incorporate a defined risk tolerance level into SLA contexts. The overall response to this question was uncertainty because data confidentiality risk is a function of threats exploiting vulnerabilities to access or obtain information assets. The findings of this study indicate that identifying data confidentiality risks expressed in SLA contexts is rare.

Based on the Delphi study data, the process of identifying and specifying a security-threat environment for each data classification and risk level is linked to the process of formulating

discrete levels of security assurance. It is noted that an appropriate level of security assurance required for mitigating each type of threat was derived from interpretations of insights from participants, as shown in Table 7.2.

Consequently, participants noted that discrete assurance levels protect against increasing sophistication of threat environment, but such assurance levels cannot indeed 'prevent' particular data confidentiality risks as listed above. However, the process of identifying data confidentiality risks ensures that appropriate data confidentiality capabilities or controls against unauthorised access are well-placed. In doing so, it helps increase trust and trustworthiness of service providers. Thus, this study implies the following principle.

Principle 2

Identifying Data Confidentiality Risks *is linked to the process of* ***Formulating Discrete Security Assurance Levels*** *in which an appropriate protection level can be incorporated into a service level agreement.*

7.3.3 Defining SLA Data Confidentiality Requirements

Grounded Theory Analysis Traceability
The theme of this subsection is linked to the following:

- SLA Data Confidentiality Requirements: Subsection 5.3.3

Defining government SLA data confidentiality requirements was defined in Subsection 5.3.3 as a process in which government agencies attempt to formulate and classify the Government's data confidentiality requirements in SLA contexts. Based on the Delphi study data, SLA data confidentiality requirements are in line with the categories of access management, data management, identity management, malicious management, compliance management. Hence, four discrete security assurance levels can be specified by using 23 data confidentiality requirements, which were derived from interpretations of insights from participants, as shown in Table 7.3.

Table 7.3: Defining SLA Data Confidentiality Requirements

SLA Requirement	Example	SAL1	SAL2	SAL3	SAL4
Access Management	access control to sensitive data		V	V	V
	limited access to sensitive data		V	V	V
	isolation from unauthorised access		V	V	V
	zero-knowledge access controls			V	V
Data Management	encrypting data during transmission	V	V	V	V
	encrypting data during storage		V	V	V
	encrypting data during processing			V	V
	key management	V	V	V	V
	adequate data classification controls	V	V	V	V
	data sharing controls	V	V	V	
Identity Management	privileges to access sensitive data		V	V	V
	single-factor authentication	V	V		
	multi-factor authentication		V	V	
	strong authentication		V	V	V
	log files and access control lists	V	V	V	V
Malicious Management	appropriate personnel security screening		V	V	V
	data leakage monitoring		V	V	V
	physical security	V	V	V	V
	risk assessment	V	V	V	V
Compliance Management	certification and attestation of suppliers	V	V	V	V
	compliance with standards and regulations	V	V	V	V
	compliance with data location requirements		V	V	V
	compliance with in-house rules			V	V

The checklist **(V)** for each SAL (Security Assurance Level) was derived from interpretations of insights from participants. Each level has distinct technical requirements for SLA data confidentiality requirements.

Overall, participants reported that government network communications were essential to be protected and controlled against unauthorised access. Moreover, participants expressed concerns about how to protect sensitive government data when using external information system services (e.g. cloud-based services), as shown in the following quotes from two representative participants.

> "*We need to establish secure government networks with a single gateway, so if there is a leak, we can know from which point*"—(P1-GOV).
>
> "*The Government should not allow sensitive government data to be stored in other countries without a strong authentication*"—(P3-GOV).

Many participants highlighted that data confidentiality requirements were necessary for formulating and classifying discrete security assurance levels. There is a relationship between SLA data confidentiality requirements and security assurance levels. However, the

fact that few previous studies attempt to investigate government SLA data confidentiality requirements. On top of that, the findings of this study indicate the importance of incorporating discrete security assurance levels in the formulation of SLAs as a means of assurance approach used to verify the security of information system services.

Review of the existing literature on security-related SLAs is undeveloped for government scenarios, especially when procuring external information system services like cloud-based services from external service providers. Consequently, an understanding of the formulation and classification of government SLA data confidentiality requirements is rare. For instance, the Government's data security requirements are traditionally expressed regarding compliance, and there is no practical evidence of any SLA data confidentiality requirements from government agencies and service providers.

Further, security-related SLAs are needed to address the Government's concerns regarding confidentiality of sensitive government data with a business model of service provisioning. The deployment of external information system services (e.g. government cloud services) will apply to security and requires new definitions of SLAs for security-relevant requirements. To this end, this study proposes the following principle.

Principle 3

Defining SLA Data Confidentiality Requirements *is linked to the process of* ***Formulating Discrete Security Assurance Levels*** *in which an appropriate protection level can be incorporated into a service level agreement.*

7.3.4 Provisioning Data Confidentiality Capabilities

Grounded Theory Analysis Traceability
The theme of this subsection is linked to the following:

- Provisions for Data Confidentiality in SLAs: Subsection 6.3.4

Providing the required data confidentiality capabilities was defined in Subsection 6.3.4 as a process in which service providers attempt to provide appropriate capabilities based

on the discrete security assurance level. Providing the required capabilities for each level is correlated with the concepts of technical provisions, physical provisions, procedural provisions and human provisions. It is note that each security assurance level can include technical, physical, procedure and human security provisions, as shown in Table 7.4.

Table 7.4: Provisioning Data Confidentiality Capabilities

Capability Provision	Example	SAL1	SAL2	SAL3	SAL4
Technical Provisions	Secure connections	V	V	V	V
	Authentication and Authorisation	V	V	V	V
	Access control	V	V	V	V
	Encryption	V	V	V	V
	Key management	V	V		
	Data isolation		V	V	V
	Malware protection	V	V	V	V
	Data breach notification	V	V	V	V
Physical Provisions	Security cages	V	V	V	V
	Access cards	V	V	V	V
	Visitor access	V	V	V	
	CCTV	V	V	V	V
Procedural provisions	Vulnerability Assessment		V	V	
	Penetration Testing		V	V	V
	Compliance with standard		V	V	V
	User access matrix		V	V	V
Human provisions	Security training		V	V	V
	Personnel security		V	V	V

The checklist **(V)** for each SAL (Security Assurance Level) was derived from interpretations of insights from participants. Each level is possible to apply the same security controls/capabilities with different levels of complexity.

The literature provides a variety of system assurances that have been used to verify the security of products, systems and services. Such criteria are often used to evaluate whether a service provider is trustworthy. This condition confirms the findings in Subsection 5.3.3.5, stating that trustworthiness of a service provider is a key driver of acceptance for most external information system services offered by service providers.

Participants highlighted the importance of trust in, and trustworthiness of, government supply chains. The majority of participants stated that trust could be achieved by looking at service provider capabilities and qualifications, such as whether service providers have certain types of technical security provisions (e.g. data encryption, data loss prevention and trusted computing). Additionally, participants stated that the Government usually validated service provider qualifications using certification and accreditation schemes. For example,

P6 reported the following statements.

> "*For data in motion, we can do encryption, using SSL, IPSec or VPN. For data at rest, we can make use of data encryption and data loss prevention, and for more advanced technologies for cloud customers, we can provide storage encryption or hardware security module*"—(P6-SP).

> "*We should comply with the ISO 27001 standard because there already has service delivery, service agreement, third party agreement, assurance, cryptography and so on. It should be enough for us to define confidentiality requirements in SLA contexts. The standard covers not only technology but also covers People and Process*"—(P6-SP).

Based on findings here, provisioning data confidentiality capabilities should be a part of the concept of formulating discrete security assurance levels. However, the notion of discrete security assurance levels as the quality of protection has not been extensively discussed in the literature. Also, few studies [33] explicitly link security to SLA capabilities.

To this end, it is essential to understand the relationships between providing the required data confidentiality capabilities and formulating discrete security assurance levels that can be incorporated into the formulation of SLAs. For example, the Government will normally not permit external service providers to process, transmit and store sensitive government data with critical risk. This is an example of the 'service provider capability' that corresponds with the data classification and risk level. Only the authorised service provider is considered trustworthy enough to provide services for handling sensitive government data. Thus, the findings of this study indicate that provisioning data confidentiality capabilities are associated with discrete levels of security assurance that implies the following principle.

Principle 4

> ***Provisioning Data Confidentiality Capabilities*** *is linked to the process of* ***Formulating Discrete Security Assurance Levels*** *in which an appropriate protection level can be incorporated into a service level agreement.*

7.3.5 Formulating Discrete Security Assurance Levels

Formulating discrete security assurance levels was defined through the Delphi study data as a process in which government agencies select an appropriate protection level to determine the level of security for services that suit government security needs, as shown in Table 7.5. In this study, formulating discrete security assurance levels is correlated with the main categories of classifying government data, identifying data confidentiality risks, defining SLA data confidentiality requirements, and provisioning data confidentiality capabilities that emerged from the Delphi study data. The statements from the participants of this study indicate that there is an association between security assurance levels and SLAs.

Overall, participants confirmed that the system availability and performance aspects were often identified as the main attributes in SLAs whereas data confidentiality requirements were typically neglected in such SLAs. The fact that almost all government agencies used the provision of the system availability to request further security capabilities to service providers, such as the availability of firewall and access controls. For example, two representative participants reported the following statements.

> "*So far existing SLAs have focused primarily on availability, while government agencies do not demand SLAs for confidentiality and integrity due to lack of awareness*"—(P31-GOV).
>
> "*In general, information security-related SLAs does not exist at all. Perhaps, characteristics of services should be defined first because each service has different security features and attributes*"—(P1-SP).

The overall response from participants to the linking of discrete security assurance levels and SLAs was positive. However, participants felt that it was difficult to measure the interplay of data confidentiality considerations that can be used to develop discrete security assurance levels. Various perspectives were expressed among both groups regarding the feasibility of security assurance levels outlined in an SLA. In this case, each level can be viewed as a set of discrete criteria that describe the characteristics of data confidentiality requirements that can be implemented by technical, physical, procedural and human security capabilities to protect sensitive government data from unauthorised access.

The notion of SLAs found in the literature is used to formulate the obligations of a service provider to deliver the agreed service according to a set of government's requirements [33]. However, many SLA provisions contain the quality of services (QoS) attributes regarding system availability and performance aspects [33] in which such QoS services typically do not include data security provisions such as data confidentiality. These findings indicate that formulating discrete security assurance levels is associated with the concepts of classifying government data, identifying data confidentiality risks, defining SLA data confidentiality requirements and provisioning data confidentiality capabilities.

A pivotal inspiration to formulating discrete security assurance levels that can be incorporated into an SLA is drawn from the NIST Electronic Authentication Guideline SP800-63 [169] and the International Society of Automation (ISA99) on security for industrial automation and control systems [73]. Such approaches relate to four levels of assurance where Level 1 is the lowest assurance level (the least resistant to threats), and Level 4 is the highest (the most resistant to threats). Each security assurance level consists of confidentiality considerations of principle 1, principle 2, principle 3 and principle 4, as shown in Table 7.5. Data confidentiality considerations presented at each level combine well with statements from the participants of this study. Notably, each security assurance level can be adjusted to cope with the increasing sophistication of the threat environment.

Further, the importance of distinct technical requirements in each discrete security assurance level is also underlined in other studies [169] [73] [170] [22]. Discrete security assurance levels play an essential role in supporting the definition and incorporation of the Government's data confidentiality requirements into an SLA. Therefore, this implies the following principle.

Principle 5

Formulating Discrete Security Assurance Levels *is linked to the process of* ***Classifying Government Data, Identifying Data Confidentiality Risks, Defining SLA Data Confidentiality Requirements and Provisioning Data Confidentiality Capabilities*** *in which an appropriate protection level can be incorporated into a service level agreement.*

Table 7.5: Formulating Discrete Security Assurance Levels

Principle	Level 1	Level 2	Level 3	Level 4
Principle 1: Classifying Government Data is linked to the process of Formulating Discrete Security Assurance Levels				
Least-Sensitive Data with Low-Risk	The technical requirements required in this level are intended for information system services processing, transmitting or storing **the least-sensitive data with low-level** , such as open government data or public data transmitted across unsecured channels and stored in public cloud services.	Technical requirements in this level are **over and above protection** for information system services processing, transmitting or storing the least-sensitive data with low-risk. However, this assured protection can be used to protect against a large scale of open government data or public data across the Internet.	Technical requirements in this level are **over and above protection** for information system services processing, transmitting or storing the least-sensitive data. Assured protection within this level can be applied to defend the least-sensitive data with low-risk, but it introduces over security protection.	Technical requirements in this level are **over and above protection** for information system services processing, transmitting or storing non-sensitive data. This level does not imply that the least-sensitive data with low-risk will not be targeted by sophisticated, advanced and persistent threat actors.
Sensitive Data with Medium Risk Level	Technical requirements required in this level are **not adequate** for information system services processing, transmitting or storing sensitive data. This level does not anticipate a higher level of threat capability that would be typical for sensitive data with medium-risk.	The technical requirements required in this level are intended for information system services (e.g. cloud-based services) processing, transmitting or storing sensitive data with restricted uses, such as personal data, email and communications and financial information.	Technical requirements in this level are **over and above protection** for information system service processing, transmitting or storing sensitive data with medium risk level, but assured protection within this level can be applied when needed and requested by customers.	Technical requirements in this level are **over and above protection** for information system service processing, transmitting or storing sensitive data with medium risk level. If implemented for this category of data and services, it is likely to be overprotected and investment.
Very Sensitive Data with High-Risk	Technical requirements required in this level are **not adequate** for information system services that process, transmit or store very sensitive data with high-risk level. This level is not intended to anticipate highly sophisticated capabilities that target this category of data.	Technical requirements required at Level 2 are **not adequate** for information system services that process, transmit or store very sensitive data. If Level 2 is implemented for this classification, it is unlikely to anticipate sophisticated threat capabilities with high resources.	The technical requirements required in this level **are applicable** for information system services (e.g. cloud-based services) processing, transmitting or storing very sensitive data with high-risk such as national economic interest and diplomatic communications.	Technical requirements in this level are **over and above protection** for information system service processing, transmitting or storing very sensitive data, but assured protection at Level 4 can be applied for this category of data when needed and requested by customers.
Most Sensitive Data with Critical Risk Level	Technical requirements required in this level are **not adequate** for information system services processing, transmitting or storing the most sensitive data. This level does not anticipate sophisticated and advanced persistent threats that would prioritise targeting the most sensitive data with critical risk level.	Technical requirements required at Level 2 are **not adequate** for information system services that process, transmit or store the most sensitive data. This level will not anticipate and defend against advanced persistent threats by the most capable state actors that would prioritise targeting the most sensitive data.	Technical requirements required at this level are **not adequate** for information system services processing, transmitting or storing the most sensitive data. Assured protection within Level 3 will not be adequate against advanced persistent threats that are specifically targeting the most sensitive data.	The technical requirements required in this level **are applicable** for information system services that process, transmit or store the most sensitive data. The most sensitive data with critical risk level will only be stored locally within national jurisdiction, such as intelligence and military data

Principle	Level 1	Level 2	Level 3	Level 4
Principle 2: Identifying Data Confidentiality Risks is linked to the process of Formulating Discrete Security Assurance Levels				
Collaborator	Level 1 is resistant to unsophisticated "collaborator" threats, with minimal capabilities and resources. Assured protection within this level will not be provided against sophisticated, persistent and blended attackers, such as organised crime and state actors.	Level 2 is resistant to sophisticated "collaborator" threats and anticipates defending data and services against compromise by a legitimate entity that provides information about the data and services to an attacker, with moderate capabilities and resources.	Level 3 is resistant to sophisticated "collaborator" threats, with high capabilities and resources. Such capabilities may be bespoke and tailored to compromise the target data and services specifically. The threat actors include organised crime and some state actors.	Level 4 is resistant to advanced persistent "collaborator" threats that prioritise compromising this category of data or service, using abundant capabilities and resources. Advanced bespoke and targeted capabilities are deployed with human sources and technical capabilities.
Exfiltration	Level 1 is resistant to unsophisticated "exfiltration" threats, with minimal capabilities and resources. This level will not provide capabilities against sophisticated, persistent and blended attackers, such as organised crime and state actors.	Level 2 is resistant to sophisticated "exfiltration" threats and anticipates defending data and services against the transmission of cryptographic keys or contents from a collaborator to an attacker, with moderate capabilities and resources.	Level 3 is resistant to sophisticated "exfiltration" threats, with high capabilities and resources. Such capabilities may be bespoke to compromise the target data and services. The threat actors include organised crime and some state actors.	Level 4 is resistant to advanced persistent "exfiltration" threats that prioritise compromising this category of data or service, using abundant capabilities and resources. Advanced bespoke for specific needs are deployed and used.
Observation	Level 1 is resistant to unsophisticated "observation" threats, with minimal capabilities and resources. Assured protection within this level will not be provided against sophisticated attackers, such as pervasive surveillance attacks.	Level 2 is resistant to sophisticated "observation" threats and anticipates an adversary to intercept or collect credentials directly from communications in an attempt to read sensitive data, with moderate capabilities and resources.	Level 3 is resistant to sophisticated "observation" threats, with high capabilities and resources. Such pervasive surveillance capabilities may be bespoke and tailored to compromise the target data and services specifically.	Level 4 is resistant to advanced persistent "observation" threats that prioritise compromising this category of data or service, using abundant capabilities and resources. Advanced bespoke and technical capabilities are deployed
Insertion	Level 1 is resistant to unsophisticated "insertion" threats, with minimal capabilities and resources. This assured protection will not be provided against a sophisticated instalment of Malware applications	Level 2 is resistant to sophisticated "insertion" threats and anticipates an adversary to inject or install a malicious program in an attempt to obtain sensitive data, with moderate capabilities and resources.	Level 3 is resistant to sophisticated "insertion" threats, with high capabilities and resources. Such technical capabilities may be bespoke to compromise the target data and services specifically.	Level 4 is resistant to advanced persistent "insertion" threats that prioritise compromising this category of data or service such as a highly capable malware, using abundant capabilities and resources.
Manipulation	Level 1 is resistant to unsophisticated "manipulation" threats, with minimal capabilities and resources. Assured protection within this level will not be provided against sophisticated and advanced persistent threats.	Level 2 is resistant to sophisticated "manipulation" threats and anticipates an adversary to manipulate someone or something to access and obtain sensitive data from the targets (e.g. people), with moderate capabilities and resources.	Level 3 is resistant to sophisticated "manipulation" threats, with high capabilities and resources. Sophisticated social engineering and impersonation capabilities may be bespoke to compromise the target data and services specifically.	Level 4 is resistant to advanced persistent "manipulation" threats with abundant capabilities and resources. Advanced social engineering and impersonation capabilities are deployed to compromise this category of data or service.

Principle	Level 1	Level 2	Level 3	Level 4
Principle 3: Defining SLA Data Confidentiality Requirements is linked to the process of Formulating Discrete Security Assurance Levels				
Access Management	There are no confidentiality requirements at this level. However, integrity and availability requirements should be managed. Access control is not required to obtain public data or information[P1-GOV]. Secure communication can be applied to prevent unauthorised access to data (or metadata).	Level 2 provides a wide range of available access control mechanisms for protecting remote connections. External access to data is regulated. Isolation mechanisms are required to prevent unauthorised access, such as virtualisation, network segmentation and trust boundaries[P6-GOV].	Level 3 requires zero access policy to very sensitive government data stored in external information system services. This level requires the isolation of the endpoint and allows the implementation of a set of firewall protections to manage incoming packets from an unclassified network[P22-GOV]	Level 4 requires zero-knowledge access controls to ensure that only the correct users access the appropriate data and services[P1-GOV]. At this level, strong authentication and authorisation rules are required to help ensure that only authenticating tenants or users access its data and resources.
Data Management	There is no encryption requirement at this level to protect data during transmission (over the network), or during storage (servers), or during processing (in memory, and operating system)[P19-GOV]	Level 2 provides encryption for secrecy, and it enables the use of standard cryptographic tools, with standardised key sizes. Keys for access are negotiated between customers and service providers[P1-GOV]	Level 3 provides strong cryptography with associated key management processes. At this level, data is managed locally, and customers encrypt keys, and customers manage keys for access[P19-GOV]	Level 4 enables the use of 'hard' crypto tools for all sensitive data and communications transmitted among parties using specialist cipher suites made by an authorised agency[P1-GOV]
Identity Management	Level 1 provides the authenticity and integrity of the transferred and storage data, and single-factor authentication and authorisation for protecting data at rest. A credential is stored and maintained by service providers[P20-GOV].	Level 2 provides timestamped signatures for authenticity, and two-factor authentication and authorisation rules for protecting data at rest. A credential is encrypted, stored and maintained by customers and service providers[P11-GOV]	Level 3 provides integrity mechanisms and time-stamped signatures for authenticity. Multi-factor authentication and authorisation are required[P21-GOV]. A credential is a zero access encrypted, stored and maintained by customers	Level 4 aims to enhance physical security by adding robust mechanisms that detect and respond to all unauthorised access. This level requires multi-factor authentication in combination with multi-factor people[P3-GOV].
Malicious Management	The best-effort physical security is required at this level to protect personnel, hardware, software, services and data from malicious physical actions. No specified measures are required to prevent rogue and surreptitious processes[P32-GOV].	Physical security is required to detect, protect and respond unauthorised attempts at physical access. A software firewall is required to manage incoming requests. Standard security measures are required to prevent insiders[P10-GOV]	Level 3 provides zeroisation, which is enabled to prevent data disclosure when the system is attached. The use of anti-tamper devices is required. This level offers protection against surreptitious compromise[P6-GOV].	Level 4 provides an 'air gap' approach, which is physically isolated from the Internet. A hardware firewall is required to manage incoming requests. Robust measures are required to prevent rogue processes and compromise by insiders.
Compliance Management	Data is allowed to be managed in remote services and stored in public cloud services. Certification is not required to demonstrate compliance with regulations[P4-GOV].	At this level, data is stored on authorised public cloud services. Certification is required to demonstrate compliance with standards and regulations[P19-GOV].	At this level, data is stored on the local server, or in private clouds. Certification and attestation of service providers are required at the human and technical level[P7-GOV].	At this level, data is managed locally and physically isolated from the Internet. Compliance with in-house rules is required to develop services for this level.

Principle	Level 1	Level 2	Level 3	Level 4
Principle 4: Provisioning Data Confidentiality Capabilities is linked to the process of Formulating Discrete Security Assurance Levels				
Technical Provisions	Service offerings may be suitable for processing, transmitting and storing the least sensitive data (Low Risk). Level 1 requires a claim of conformity, which is determined based on the services they are offering according to the technical provisions at Level 1.	Service offerings may be suitable for processing, transmitting and storing sensitive data (Medium Risk). Level 2 requires a claim of conformity, which is determined based on the services they are offering according to the technical provisions at Level 2.	Service offerings may be suitable for processing, transmitting and storing very sensitive data (High Risk). Level 3 requires a claim of conformity, which is determined based on the services they are offering according to the technical provisions at Level 3.	Service offerings may be suitable for processing, transmitting and storing the most sensitive data (Critical Risk). Level 4 requires a claim of conformity, which is determined based on the services they are offering according to the technical provisions at Level 4.
Physical Provisions	Service offerings may be suitable for processing, transmitting and storing the least sensitive data (Low Risk). Level 1 requires a claim of conformity, which is determined based on the services they are offering according to the physical provisions at Level 1.	Service offerings may be suitable for processing, transmitting and storing sensitive data (Medium Risk). Level 2 requires a claim of conformity, which is determined based on the services they are offering according to the physical provisions at Level 2.	Service offerings may be suitable for processing, transmitting and storing very sensitive data (High Risk). Level 3 requires a claim of conformity, which is determined based on the services they are offering according to the physical provisions at Level 3.	Service offerings may be suitable for processing, transmitting and storing the most sensitive data (Critical Risk). Level 4 requires a claim of conformity, which is determined based on the services they are offering according to the physical provisions at Level 4.
Procedural Provisions	Service offerings may be suitable for processing, transmitting and storing the least sensitive data (Low Risk). Level 1 requires a claim of conformity, which is determined based on the services they are offering according to the procedural provisions at Level 1.	Service offerings may be suitable for processing, transmitting and storing sensitive data (Medium Risk). Level 2 requires a claim of conformity, which is determined based on the services they are offering according to the procedural provisions at Level 2.	Service offerings may be suitable for processing, transmitting and storing very sensitive data (High Risk). Level 3 requires a claim of conformity, which is determined based on the services they are offering according to the procedural provisions at Level 3.	Service offerings may be suitable for processing, transmitting and storing the most sensitive data (Critical Risk). Level 4 requires a claim of conformity, which is determined based on the services they are offering according to the procedural provisions at Level 4.
Human Provisions	Service offerings may be suitable for processing, transmitting and storing the least sensitive data (Low Risk). Level 1 requires a claim of conformity, which is determined based on the services they are offering according to the human provisions laid down at Level 1.	Service offerings may be suitable for processing, transmitting and storing sensitive data (Medium Risk). Level 2 requires a claim of conformity, which is determined based on the services they are offering according to the human provisions laid down at Level 2.	Service offerings may be suitable for processing, transmitting and storing very sensitive data (High Risk). Level 3 requires a claim of conformity, which is determined based on the services they are offering according to the human provisions laid down at Level 3.	Service offerings may be suitable for processing, transmitting and storing the most sensitive data (Critical Risk). Level 4 requires a claim of conformity, which is determined based on the services they are offering according to the human provisions laid down at Level 4.

7.4 Validation of the proposed Framework

This thesis uses approaches for validating foundations for a TDSLA capability framework, namely: 1) reflection on related works; 2) testimonial validity; and 3) applications of transferability.

7.4.1 Reflection on related Frameworks

The SPECS (Secure Provisioning of Cloud Services based on SLA management) framework conducted by European communities [28] is one of the contributions to the field. As part of their research, SPECS has proposed an open source framework to offer security-as-a-service, by relying on the notion of security criteria specified in SLAs. The SPECS framework addresses both cloud service providers and cloud service customers to provide techniques and tools for enabling negotiation, monitoring and enforcement of security criteria in cloud SLAs. SPECS also offers tools to help cloud service providers and cloud service customers to verify the security assurance through Security SLAs which are based on standard security controls, such as CSA Cloud Control Matrix, NIST 800-53 Rev.4 and ISO/IEC 27017 – Information security controls for cloud services.

Compared to the SPECS framework, the TDSLA capability framework that emerged from the Delphi study data aims at certifying levels of security for services by incorporating discrete security assurance levels into SLA contexts. In a similar vein to SPECS, security assurance levels are linked to the security requirements of customers and security capabilities provided by service providers. However, the four discrete levels of increasing security assurance allow for cost-effective solutions that are appropriate for various information system services that process, store or transmit government data. The framework enables government agencies to select an appropriate security assurance level based on the data classification and risk level. Government agencies can make use of the framework to procure and use cloud-based services by determining an appropriate level of protection according to their security needs and requirements.

Similarly, the multi-cloud secure applications (MUSA) framework is developed to support the security-intelligent lifecycle management of distributed multi-cloud applica-

tions [29]. MUSA extends the Security SLA of SPECS with additional features. The MUSA framework is developed to detect violations of such composite Security SLA. MUSA offers an integrated tool to monitor and enforce the secure behaviour stated in the Security SLA of the multi-cloud application [102].

Compared to the MUSA framework, the findings of this study have proposed a TDSLA capability framework as a means of incorporating the Government's data confidentiality requirements into an SLA between government agencies and service providers. The TDSLA capability framework aims at facilitating an improved understanding between government agencies and service providers when using cloud-based services to process, transmit or store sensitive government data. In other words, the TDSLA capability framework is a pragmatic approach that can be adopted by any government ministry, agency or department when using external service providers to process, transmit, and store government data or operate government's information systems on behalf of the Government.

Likewise, the SLA-ready framework is developed to provide a reference model for developing cloud SLAs and a set of digital services to support cloud service customers in the use of SLAs [30]. The SLA-ready reference model is developed based on standard specific requirements, including functional, non-functional, security, data protection, legal and business requirements. The SLA-ready framework makes use of security controls from the CSA Cloud Control Matrix and the ISO/IEC 19086 standard on Cloud Computing Service Level Agreement Framework to specify security and privacy policies in SLA contexts. The TSDLA framework developed from this research purposely does not aim to incorporate security controls into contracts or SLAs directly. However, this study formulates and classifies security controls into discrete security assurance levels to better protect sensitive government data against unauthorised access.

The above studies presented thus far provide evidence that there is a growing awareness and application of security-related SLAs in practice. Based on understanding from such studies, incorporating standard security controls (e.g. NIST 800-53 and ISO/IEC 27002) into contracts or SLAs constitute security-related SLAs. However, the importance of certifying levels of security for services is still not adequately considered when the Government using external information system services for processing, transmitting or storing sensitive data.

To this end, developing a TDSLA capability framework is intended as a means to incorporate the Government's data confidentiality requirements into an SLA through selecting an appropriate discrete security assurance level that is believed to be capable of preserving data confidentiality within a defined risk tolerance level in an SLA. The key reasons for defining the various levels are: 1) to find distinct levels where one can make an objective judgement about which level's criteria are met; and 2) to make the difference between levels qualitatively distinct regarding the classes of threats which they address or mitigate. Without such fundamental models, there are only limited options available with simple binary assessment (compliance or noncompliance) on security which appears to be too coarse for complex security environments. Further, the binary assessment seems problematic for most practitioners and policymakers to comprehend and compare clearly.

Further, building a TDSLA capability framework is inspired by the adaptability of the CC certification process. CC aids to build trust through two main components, namely: protection profiles; and evaluation assurance levels (EALs). A protection profile specifies a set of security requirements for a specific type of product. Unlike protection profiles, the EAL level does not show the actual security capabilities of the product, but independently evaluates the product as evidence of adequate testing against the security target. In other words, the CC aims to certify levels of security for products while the TDSLA capability framework aims to certify levels of security for services.

In the same vein, developing foundations for a TDSLA capability framework consists of two main components, namely: discrete assurance levels; and service level agreements. A discrete level of assurance defines a standard set of data security requirements for specific types of threats and data classification levels. In addition to discrete assurance levels, the use of service level agreements is intended to examine a service provider's capabilities to meet the customer's data security requirements and to agree with the requirements and provide the required level of security assurance between parties.

Therefore, these are the reasons to construct better assurance mechanisms in service provision that give government agencies as much transparency and confidence as possible that any sensitive government data transferred to service providers is processed, stored and transmitted securely. In addition, the framework is easy to use without deep expertise.

Service providers are required to provide evidence that the service they are offering can potentially demonstrate agreed security assurance levels. A government tender could review whether the service provider capabilities are in line with technical requirements for the required level of assurance.

7.4.2 Testimonial Validity

Testimonial validity refers to the accuracy of the interpretations made by the researcher by checking whether the principles and framework that emerged from the Delphi study data are convincing to participants from the Government and service providers [138, 144, 146]. In this study, the researcher provided the opportunity for the participants to comment on the principles and framework obtained from the Delphi study data. All 50 participants were invited to participate in the validation; 19 participants responded. The principles and framework were assessed by the participants using a five-Likert scale questionnaire and open-ended questions. An iterative process of definition and validation of principles and framework was conducted by using the participants' feedback. It is important to note that the aim is not to estimate the distribution of participants' opinions. Instead, it is an attempt to have early information about expected completeness and usefulness of the principles and framework.

The results of validation are positive in general, and a majority of the participants agree with the principles and framework that emerged from the data. Note that positive opinions of participants may be motivated by a desire to finish the feedback quickly or to be kind to the researcher. Negative or critical views of participants, on the other hand, are also beneficial, especially if the participant can indicate which element of the principles and framework would not be useful in real-world contexts. These factors were addressed by quantitatively assessing feedback. In this thesis, the evaluation feedback aimed at providing minimum 70% agreement from the participants to support validation of principles and framework [110]. Thereby, participants confirmed the correctness and practicability of the findings that emerged in the research, even though the summarised results did not necessarily reflect every single opinion and statement.

Finally, the researcher asked participants to review the framework that emerged from this study regarding the completeness and the usefulness of the framework. It was essential to identify if the proposed framework is consistent with government needs. The findings identify consistencies with the participants' expectation.

> "*Overall this framework seems pretty consistent with what I have observed, and the framework has better described the real needs* " (P02).

Adding that,

> "*From theoretical and normative perspectives, the framework is suitable and correct. However, It needs to be applied in the real-world contexts* " (P11).

> "*The framework has defined an appropriate standard for the Government. However, it needs further work to implement it*" (PG12).

Furthermore, one participant suggested that the completeness of the framework was :

> "*the need for the inclusion of data integrity and non-repudiation requirements in the framework, as well as the better classification of health data* " (PG03).

In addition to this, one participant (PG07) suggested to include safety and facility factors in the formulation of SLAs. Another participant (P08) indicated that the completeness of the framework was the inclusion of human security factors in the SLA framework.

Regarding the usefulness of the framework, it is essential to identify the usefulness of the framework from different perspectives. All of the participants generally recognised the value of the framework for the Government when procuring and using external information system services offered by service providers.

> "*I think it could be somewhat useful for government and you have done the potential to be a really good framework, and this is important to be doing*" (PG05).

Adding that,

> "*I think it could something that can be implemented in government and public organisations*" (P02).

In summary, 19 participants were asked to evaluate the framework for its completeness and usefulness. Regarding the completeness, there were a few inconsistencies identified between the principles and framework and the participants' perceptions. All of the participants identify the usefulness of the framework. While there was agreement about the usefulness of the framework a number of suggestions were made to expand the scope of the framework. For example, how the framework can be used to support government procurement for services that process, transmit or store sensitive government data. This leads to a need for further research to evaluate the data classification levels in more detail for discrete security assurance levels.

7.4.3 Applications of Transferability

Transferability refers to the degree to which the proposed framework emerged from the Delphi study data can be applied in other contexts or settings. Due to the nature of qualitative studies, the possibility of generalising the framework is limited. Thus, the framework will be applied to a specific context such as Amazon Web Services - UK Government Cloud (AWS-G Cloud) and AWS-the US Federal Risk and Authorization Management Program (AWS-FedRAMP) to show the applicability of the findings of this study.

7.4.3.1 The UK G-Cloud Framework

The UK-Government Cloud (G-Cloud) is one of the most extensive cloud government procurement frameworks. The G-Cloud consists of framework agreements with cloud service providers and the digital marketplace which allow government and public sector organisations to search for cloud services that are listed in the G-Cloud Framework. Government agencies can procure and purchase cloud services listed on the digital marketplace without calling for a full tender process [171].

For example, government agencies can procure and use global cloud services, such as AWS which is listed on the G-Cloud framework [58]. At that stage, security accreditation is required for for organisations such as AWS that want to provide services to government agencies. In this case, AWS is considered as assured public cloud services, which are

subjected to the ISO 27001 certification and other certifications. Although AWS is listed within G-Cloud, such a service is unlikely to be appropriate for most official information in which data and services must be hosted in the UK [89]. The use of AWS services may be appropriate for non-sensitive official information.

On top of that, the process of security accreditation was slow, costly and very resource-intensive. Consequently, the accreditation process was replaced by a self-assertion process within the G-Cloud 9 framework. In doing so, AWS is required to complete many defined security statements asserting how their services meet the Cloud Security Principles.

The Cloud Security Principles cover the following 14 key areas: data in transit protection; asset protection and resilience; separation between customers; governance framework; operational security; personnel security; secure development; supply chain security; secure customer management; identity and authentication; external interface protection; secure service administration; audit information provision to customer; and secure use of the service by the customer [62].

Each principle represents a fundamental security aspect that should be considered when selecting cloud services. Service providers are contractually bound to truthfully complete specific security functionality, which can be used to satisfy such principles. In this case, AWS is expected to consider the 14 Cloud Security Principles and to provide the required security assurance of these principles when delivering services to government agencies. The G-Cloud framework allows government agencies to make informed choices about which services are appropriate for their needs and requirements. Also, AWS is required to provide evidence to support their assertion to government agencies for evaluation.

For instance, data in transit protection is one example of a cloud security principle that focuses on the confidentiality of data. Security controls are implemented via a combination of network protection and encryption [62]. In [172], AWS provides security capability against network attacks, such as via a secure sockets layer (SSL) protected against the man in the middle (MITM) attack. Concerning data encryption in transit, AWS also supports protecting data in transit via both SSL/TLS (Transport Layer Security) and IPSec, which is subjected to compliance with ISO 27001, PCI-DSS, SOC 1, SOC 2 and SOC 3.

Further, AWS heavily relies on certification schemes, such as Cyber Essential Plus, FedRAMP, FIPS, ISO 27001, ISO 27017, ISO 27018, PCI DDS, SOC 1, SOC 2 and SOC 3. The service provider claims to be compliant with applicable laws including HIPAA, UK Data Protection Act, EU General Data Protection Regulation, Privacy Act (Australia), Privacy Act (New Zealand), Personal Data Protection Act (Malaysia), Personal Data Protection Act (Singapore) and Personal Information Protection and Electronic Documents Act (Canada). AWS has also demonstrated alignment with many security frameworks including CIS (Centre for Internet Security), CJIS (Criminal Justice Information Services), CSA (Cloud Security Alliance Controls), NIST, G-Cloud, and Cloud Security Principles [27].

Within the G-Cloud framework, six common approaches can be used to address several cloud security principles, namely: service provider assertion; contractual agreements; independent validation of assertions; independent testing of implementation; assurance in the service components; and assurance in the service design [62]. The self-assertion approach developed under G-Cloud is far more practical. In the same vein, the use of TDSLA capability framework is feasible in this context. Cloud service providers are required to go through a set of discrete security assurance levels, which are determined based on the service they are offering, and provide self-assertion of compliance.

In addition to self-assertion, the use of service level agreements is a means to examine a service provider's capabilities to meet the customer's security requirements and to agree on a level of security assurance between parties. Various levels of security assurance can help steer government agencies and service providers towards the compliant adoption of cloud services. The simplification of data classifications scheme and risk assessment can help making transparency and accountability more feasible how government data is to be processed, transmitted or stored.

In comparison, the TDSLA framework allows agencies to decide which of the services are most suitable for handling government data, and which security assurance level they require in the provision of the selected services. Service providers that want to include their cloud services within the framework are required to submit the specific service they want to supply, and they need to specify a claim of conformity against a specified level of security, which is determined based on the services they are offering to government agencies.

The UK Government is required to conduct an assurance review of the service providers to be accepted into the digital marketplace. Further, the government can create framework agreements with service providers by using discrete security assurance levels. The formulation of data confidentiality requirements is necessary to avoid ambiguity about which an appropriate level of security assurance a customer requires. Identifying and incorporating discrete security assurance levels into SLA contexts are essential to quantify and guarantee a defined risk tolerance level based on the data classification and threat environment.

7.4.3.2 The US FedRAMP Framework

The Federal Risk and Authorization Management Program (FedRAMP) [173] [64] is a US government framework that carries out a standard approach to the security assessment, authorisation, and continuous monitoring for cloud services. Cloud service providers whose services are currently being used by the US government or are interested in offering their cloud service to the federal government should obtain a FedRAMP authorisation. FedRAMP makes use of the NIST 800-53, Rev. 4 security control baseline for moderate or high impact levels. The framework requires cloud service providers to receive an independent security assessment conducted by a third-party assessment organisation to ensure that authorisations are compliant with the Federal Information Security Management Act (FISMA).

FedRAMP is required for any cloud service provider seeking to work with federal agencies. The use of FedRAMP aims to increase transparency between the US Government and cloud service providers especially for consistency and confidence in the security of cloud services using NIST and FISMA standards. For instance, the Cloud First Policy requires all US federal agencies to use the FedRAMP process to conduct security assessments, authorisations, and continuous monitoring of cloud services [174].

Once a service provider has been authorised, it is listed in the FedRAMP marketplace. Federal agencies can find cloud services that meet their needs. Knowing that any services listed in the marketplace have been authorised and meet security requirements, federal agencies can review the existing authorisation package to use the service. This framework prevents the government and the service provider from duplicating work. In other words, it can be used many times when a cloud service provider has been authorised once.

Regarding the application of the FedRAMP framework, AWS has become a FedRAMP Authorized Cloud Service Provider in which AWS has addressed the FedRAMP security controls and has been assessed by an accredited independent third-party assessor. Within the framework, ASW is required to maintain continuous monitoring requirements of FedRAMP. For example, AWS GovCloud (US) has been granted a Joint Authorization Board Provisional Authority-To- Operate and multiple Agency Authorizations for high impact level while AWS US East-West has been granted for moderate impact level. Notably, AWS GovCloud (US) [164], which is designed for the US government and its partners, has achieved DoD (Department of Defense) impact level 5 Provisional Authorisation. Such level accommodates controlled unclassified information (CUI) that requires a higher level of protection.

It is clear that that AWS is trustworthy enough to be used for US government agencies through AWS GovCloud, which is a private cloud service to hosted sensitive government data and only operated solely by employees are vetted US Citizen before being granted access credentials to the region [164]. One reason for this is that over 2000 government agencies including US Department of State, US Centers for Disease Control and Prevention, US Food and Drug Administration and NASA Desert Research and Training Studies make use of AWS services [164].

However, such a process is particularly complex where cloud service providers are reliant on an independent third party assessment organisation. Additionally, obtaining such certification and accreditation is a bureaucracy process, and there is a need for further time and costs for service providers, which may result in increased prices. The application of FedRAMP also requires significantly more effort and pre-established security infrastructure [64].

On top of that, the self-assertion approach developed under the TDSLA capability framework seems to be more practical and feasible in this context. Cloud service providers that are interested in providing cloud services to US federal government agencies are required to go through a set of discrete assurance levels, which are determined based on the service they are offering, and provide self-assertion of compliance.

Furthermore, the use of service level agreements is intended to examine a service provider's capabilities to meet the government's data security requirements and to agree on the required and provided a level of security assurance between parties. The simplification

of the framework is to propose four discrete security assurance levels that help steer federal agencies towards the compliant adoption of cloud services. Also, the formulation of the data classification scheme applied in each assurance level has helped make it more transparent how sensitive government data is to be processed, transmitted or stored.

More generally, the applicability of TDSLA capability framework allows government agencies to decide which of the services are most suitable to procure, and which level of assurance they require in the provision of the selected services. Within the TDSLA framework, cloud service providers are required to submit the service they want to supply, and they specify a claim of conformity against a specified level of security assurance, which is determined based on the services they are delivering to government agencies. In doing so, the Government is required to conduct an assurance review of the service providers to be accepted into the digital marketplace. In addition to this, Government agencies can make a business relationship with service providers through an SLA using discrete security assurance levels.

7.4.4 Discussion

The TDSLA capability framework is intended to provide a practical and reliable evaluation of the security capabilities of information system services. By providing self-assertion of compliance of a service's ability to meet security assurance level, the proposed framework gives customers, such as government agencies, more transparent and confidence in the security of information system services which, in turn, leads to more informed decisions. Government agencies increasingly require certifying levels of security for services as a determining factor in purchasing decisions. Since the requirements for each discrete security assurance level are established, service providers can target particular security needs and requirements while providing information system services (e.g. cloud services).

Evaluating a service for security requires identification of the customer's security needs and an assessment of the capabilities of service providers that offer services. The proposed framework aids customers in both of these processes through two key components: discrete security assurance levels and service level agreements. A discrete security assurance level

defines a standard set of data security requirements for a specific type of service. The value of the discrete security assurance levels comes from the idea that any objective observer will agree about what level is achieved by a particular service. In other words, it is necessary to have clarity about what characterises the different levels for each data classification and threat environment. Ideally, customer expectations should be transparent in legal language. Hence, these levels of agreement can form the basis for constructing legal language in contracts or SLAs.

Further, by listing the required level of assurance for service families, the proposed framework allows a service provider to state conformity to a relevant level of security assurance, which is determined based on the services they are offering to government agencies. For example, a service provider that is intended to process, transmit and store general personal data (e.g. name, date of birth, national identity) is required to go through security assurance level 2 (SAL2). On the other hand, if the service offered by a service provider process, transmit and store specific personal data (e.g. Biometric), a service provider is required to state conformity to security assurance level 3 (SAL3). In other words, the service is tested against a specific level of security assurance, providing reliable verification of the security capabilities of the service. Since the security of information system services can be linked to a particular security assurance level, customers can assess a list of security requirements and features by examining the details of a relevant level of security assurance. Also, customers can determine the service's ability to meet their security needs, and compare the security capabilities of any other services.

Based on the findings, the TDSLA capability framework is developed to facilitate how to incorporate the Government's data confidentiality requirements into an SLA. One benefit of using such a framework is that the ability of the framework to include discrete security assurance levels, which are determined based on the service they are offering. This framework has allowed service providers to deliver an appropriate level of security assurance in the provision of procured services. Moreover, this leads to a simple means of incorporating the Government's data confidentiality requirements into an SLA between government agencies and service providers by allowing government agencies that do not have the technical knowledge to specify government security needs merely.

An essential decision in the formulation and classification of the Government's data confidentiality requirements into discrete security assurance levels was the need to ensure the simplicity and clarity of the application of the proposed framework. The aim is to provide sufficient practical knowledge to novice staffs without requiring them to learn how to classify data confidentiality requirements and capabilities according to types of threats or vulnerabilities. Therefore, government agencies that possess deficiencies in identifying the required the Government's data confidentiality requirements and capabilities can select an appropriate service provider that offers the level of security assurance required to protect sensitive government data, thereby improving the overall quality of government procurement of external information system services.

The need for expressing the discrete levels of assurance in the form of SLAs has been considered as the most effective means of assuring service scenarios because it is useful in avoiding ambiguity regarding what is being expressed and performed by service providers. In this thesis, discrete assurance levels are practical ways of classifying the Government's data confidentiality requirements according to a set of threats at each of government data classifications. Therefore, discrete levels of assurance play an essential role in support of defining and enforcing the Government's data confidentiality requirements in SLA contexts.

Some examples of the security assurance levels are presented in the context of a government cloud in the following requirements: access management, data management and malicious management.

7.4.4.1 Requirement 1: Access Management

If the Government decides to lease network infrastructure from external service providers, the Government would need to ensure that the network segmentation and segregation meet the minimum security requirements, which can be specified in SLAs. To defend against the most serious threats, some potential SLA attributes for isolation mechanisms, such as whitelisting, virtual LANs, traffic flow filters for web and email, and 'air-gap', should be specified in the formulation of security-related SLAs. Although a true 'air-gap' seems to be used in an environment that sensitive government data is not connected to a network, it is, of course, unrealistic to represent this approach when using cloud-based services.

It is acknowledged that cloud-based services remove the concept of the 'air-gap' approach. However, data and network isolation need to be considered carefully to achieve as much of a security requirement as possible in SLAs. For example, most virtual machines run on the same physical hardware that leads to sharing the underlying infrastructure with untrusted customers. However, common access control and security policies are not sufficient to assure isolation in cloud data centre services. Thus, isolated networks at Level 3 may provide an acceptable level of protection against unauthorised data disclosure from trusted to untrusted cloud-based services. Overall, **Security Assurance Level 3** may be suitable for this case. It is expected that this level of security precautions can mitigate the threats at least to increase the efforts required to access sensitive government data.

Such usage contexts above confirm that the application and development of government cloud require to achieve a high level of assurance (**Security Assurance Level 3**). On top of that, the framework presented is clearly in need of further elaboration through application to a wider range of services. A complete description of the framework will adequately describe the protections achieved and threats mitigated by each level of security assurance. This framework could help to match security assurance level to services and to identify 'clusters' of services with similar security concerns. However, there is no simple progression from 'low-security assurance' services to 'high-security assurance'. This is because some of higher discrete levels of security assurance require technical insights along with further research challenges. It is expected that by defining interesting areas, this study may stimulate discussion on how to achieve such certifying levels of security for services.

7.4.4.2 Requirement 2: Data Management

Increasing amounts of sensitive government data require cryptographic tools for ensuring data confidentiality or data integrity. The use of cryptographic technologies appears to be of limited interest as it is reliant on standard solutions. Thus, the Government should understand which sensitive information needs to be protected to decide whether cryptographic technologies will be deployed (in-house or out-sourced) at the application level, file system level, network level, or device level. Also, the Government would need to ensure that cryptographic tools are appropriately configured, as the proper implementations of cryptographic

technologies are incredibly critical to their effectiveness against the unauthorised disclosure of sensitive government data. Thus, it is necessary to understand whether data is managed locally, or in remote services when one defines security attributes in SLAs.

Furthermore, when the Government decides to use cloud-based services from external service providers, it is essential to understand whether data is encrypted by service providers or by end-users or keys for access negotiated between a user and a service provider. It is evident that the absence of attributes for cryptographic key management in the formulation of security-related SLAs makes it impossible for cloud service providers to meet the increasing demand for data security as well as to offer trustworthy services to their customers.

Of course, key management is critical and challenging in a cloud environment. Cloud-based services can provide a secure connection using TLS or SSH. Like traditional data centres, cloud data centres also can store application data in an encrypted form. If the Government requires high data confidentiality requirements, cloud service providers can provide end-to-end encryption. In this case, cloud service providers are required to provide evidence to demonstrate that they do not have access to the encryption keys or they would not be able to hold those keys over unauthorised entities. Thus, the need for third-party vendor protection requirements would be required to be built into contracts or SLAs, as most services or applications store data in cloud data centres. One also needs to look at the entire data supply chain when data is stored in multiple locations and in what country the data is stored. Overall, in the context of a government cloud, the specified levels of assurance will be appropriate at **Security Assurance Level 3**.

7.4.4.3 Requirement 3: Malicious Management

It is necessary to include physical security attributes in the formulation of security-related SLAs through security assurance levels. In practice, many cloud service providers claim that they have 24 x 7 x 365 services on-site physical security to protect against unauthorised entry, which can be checked through security audits to help build the trust and confidence between a customer and a service provider [96]. Physical security controls can include security guards, physical access control devices (e.g. locks), physical intrusion alarms, and surveillance types of equipment (e.g. CCTV) [1].

Further, the physical location of cloud data centres has been highlighted as a significant concern since the Edward Snowden revelations in 2013. Although data security does not only depend on its geographical location, many governments are not allowed to store citizen's data under other jurisdictions. For instance, according to Article 17 of the Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, mentioning that Electronic System Operators have obligations to locate data centres within the borders of national jurisdictions, especially for law enforcement and protecting citizen's data against force majeure (e.g. earthquakes, floods and wars) [175]. In particular, localised data centres may help to get access, as well as to apply digital forensics to cloud-based services for law enforcement. Therefore, it is essential to include the physical location of data centres in the formulation of security-related SLAs when using cloud-based services provided by external service providers, especially for processing, transmitting and storing sensitive government data. In the context of a government cloud in general, this corresponds to **Security Assurance Level 3**.

In summary, the principles and framework formulated during this study are summarised in Table 7.6 by giving details on five related aspects: 1) understanding based on findings and literature; 2) proof of quotations (random selection); 3) reflection against related work; 4) agreement to support validation on the derived principles and framework; and 5) position of applicability.

7.5 Chapter Summary

This chapter has developed a set of principles as foundations for a TDSLA capability framework. Such principles include the activities of classifying government data, identifying confidentiality risks, defining government SLA confidentiality requirements, provisioning data confidentiality capabilities and formulating discrete security assurance levels. Three approaches have been used to validate the principles and framework. Reflection against related works has been performed to compare with the existing literature. Furthermore, a validation of the principles and framework has been conducted through exercising the principles and framework using the participants' feedback. This chapter has also discussed

the proposed framework with two real cases to show the applicability of the framework, using AWS G-Cloud and AWS-FedRAMP as a trusted cloud provider for many governments. Such real-world examples are expected to contribute to the improvement of the applicability of a TDSLA capability framework.

Table 7.6: Understanding, Proof, Agreement, Reflection and Position

	A TDSLA Capability Framework	**Principle #1: Classifying Government Data**	**Principle #2: Identifying Confidentiality Risks**
Understanding based on findings and literature	Incorporating standard security controls like NIST 800-53 and ISO/IEC 27002 into SLAs constitute security-related SLAs. However, these approaches do not incorporate data confidentiality requirements into SLAs according to data classification and threat environment.	Any parties who work with the Government have to ensure such sensitive data is appropriately protected under the Government's requirements. However, there is little recognition of the level of assurance expressed in SLAs according to data classification and threat environment.	There is little recognition of incorporating data confidentiality risks, which are mitigated by each discrete level of security assurance. A service provider may conduct a risk assessment, concerning a distinctive level of security assurance. Each level protects against different threats.
Proof Quotation for the principles and framework presented in figure 7.2 (random selection)	"*Existing SLAs have focused primarily on availability, while customers do not demand SLAs for confidentiality and integrity due to lack of awareness* (P31-GOV)" "*In general, information security-related SLAs does not exist at all. Perhaps, characteristics of services should be defined first because each service has different security features and attributes*" (P1-SP)	"*Regarding data, classifying data is necessary to define in the first place. Also, we need to understand whom the information owner allowed access*" (P5-SP) "*Each ministry should classify its data as public, regulated, restricted, secret and top secret. However, the classification of confidential data in Ministry A may be different classification with ministry B*" (P19-GOV)	"*Regarding key management, our customer can hold the encryption keys, even though the encryption process has been created at the provider side*" (P1-SP) "*Actually, threats and attacks can come from inside government networks, such as our observation discovered botnets keep sending out the data*" (P13-GOV)
Reflection against related works	The SPECS Framework [28], The MUSA framework [29] and SLA-Ready [30]. Overall, the importance of SLAs-based on discrete levels of assurance is still not fully considered when service providers are handling sensitive data. The key inspiration and reference point for building a TDSLA capability framework is the CC certification process.	Data classification for cloud readiness [176], Government Security Classification [89]. The existing literature does not focus on the data classification level that can be expressed in SLA contexts. There may be other data management constraints over sensitive government data (e.g. data protection, national security and health regulation)	Assurance levels against threats [22, 169, 170], Risk Management [29], Threat Analysis [29]. In short, the existing literature does not identify the linkage between threat mitigation and an appropriate level of security assurance incorporated into SLA contexts. Each level is expected to have different capabilities against threats.
Agreement to support validation	100%	94.7%	94.7%
Position of applicability	The framework can be applied to a specific context such as Amazon Web Services - UK Government Cloud (AWS-G Cloud) and AWS-The Federal Risk and Authorization Management Program (AWS-FedRAMP) to show the applicability of the framework.	Classifying government data can be expressed in the formulation of assurance-based SLA. Thus, this principle can be used to encourage lucidity and characterise certain levels of protection ranging from the lowest level of assurance to the highest level.	This principle can help to quantify a defined risk tolerance level for each level incorporated into SLAs. The identification of perceived confidentiality risks is essential to avoid ambiguity about which an appropriate level of assurance a customer requires.

	Principle #3: Defining SLA Data Confidentiality Requirements	**Principle #4: Provisioning Data Confidentiality Capabilities**	**Principle #5: Formulating Discrete Security Assurance Levels**
Understanding based on findings and literature	Defining government SLA data confidentiality requirements is necessary to delineate the quality of protection or an appropriate discrete security assurance expressed in SLAs. This context raises questions on whether data confidentiality can be adequately expressed in SLA contexts.	The quality of protection is measured according to the confidentiality capabilities of a service provider to deliver the agreed service based on a set of data confidentiality requirements. Provisioning data confidentiality capabilities are different for each level of security protection.	There is little recognition of discrete security assurance levels expressed in SLAs. Whereas, there is a need to incorporate specific security clauses into an SLA-based discrete security assurance level that defines a standard set of data security requirements against unauthorised access.
Proof Quotation for our principles and the framework presented in figure 7.2 (random selection)	"*we have to create a single entry point for government secure communications and networks so that should there is any leak, we can easily find it out*"(P1-GOV). "*the Government should not allow any sensitive government data to be stored and hosted in other countries without extra security controls taken place, such as a strong password*" (P3-GOV).	"the highest level, there is a tamper-proof mechanism, if there is a rigorous attempt to obtain sensitive data; this can perform active zeroisation" (P6-GOV) "*we can encrypt data in transit, using VPN, SSL, and IPSec. We can use storage encryption and DLP for protecting data at rest, we can provide a hardware security module for customers*" (P4-GOV)	"*Existing SLAs have focused primarily on availability, while customers do not demand SLAs for confidentiality and integrity due to lack of awareness*" (P31-GOV) "*Security-related SLAs does not exist at all. Perhaps, characteristics of services should be defined first because each service has different security features and attributes*" (P1-GOV)
Reflection against related works	UK Cloud Security Principles [62], Security Requirements for protecting the confidentiality of CUI [47]. Based on the literature, we deepen the understanding by providing insights into government SLA data confidentiality requirements that are investigated in this study.	Introduction to AWS Security capabilities [177], Meaningful Security SLAs [32], Building Security SLAs [35]. Building upon the knowledge of previous studies we deepen the understanding of incorporating a service provider's data confidentiality capabilities into SLA contexts.	Security SLAs for Federated Cloud Services [33], Quality of Security Services [178], Security SLAs [167], NISTSP800-63 [169], ISA99 [73]. There appears to be an insufficient investigation into incorporating the Government's data confidentiality requirements in SLAs.
Agreement to support validation	84.2%	89.5%	100%
Position of applicability	This principle has significant implications for providing useful guideline when formulating discrete levels of assurance. Each level has a different level of SLA confidentiality requirements.	This principle is necessary for guiding for delivering the required confidentiality capabilities for each level of assurance, and it is beneficial to incorporate such provisions into SLA contexts.	This principle can be used for the formulation of SLA-based discrete levels of assurance that play an essential role in supporting the definition and enforcement security considerations in SLA contexts.

8
Conclusions

> *The important thing is to never stop questioning. No problem can be solved from the same level of consciousness that created it.*
>
> Albert Einstein,

Contents

8.1 Summary

Many government agencies rely on certification schemes as a means of assuring to demonstrate that products, systems and services have met industry standards for security. While this is useful, problems have been identified with the applications of certification schemes [15, 18, 19, 23, 24]. Many authors claim that certification schemes do not provide the level of security assurance required to ensure sufficient security of products, systems and services that are currently available in the marketplace. More specifically, certification schemes are known to be slow-moving processes, and not well-suited to the service scenario because they are designed for a static scenario where protection profiles are developed based only on the assumptions about the target environment [24]. Additionally, such certification processes are mostly manual and require considerable efforts and investment [26]. Therefore, assurance-based certification does not scale well to support a dynamic service environment [26], such as cloud-based services.

Notably, the findings of this study reveal that service providers are very dependent upon certification schemes to provide security guarantees to customers or government agencies. In the context of Indonesia, the certification scheme used is limited to the application of the ISO/IEC 27000 series standards. From a global perspective, cloud service providers such as Amazon and Microsoft have used various certification schemes to assure security for the services provided to their customers, and demonstrate their services compliance with ISO, PCI, DoD or FedRAMP [27]. The problem here is that such certification schemes offer only a binary assessment (secure or insecure) or (compliant or non-compliant). Additionally, the level of security assurance required does not incorporate well into SLA contexts.

There has been some research into expressing security parameters in SLA contexts as a means of addressing the limitations of certification schemes [28–30]. The approach taken by previous research is to incorporate security controls into the scope of SLAs. While such studies provide valuable insight into the problem of formulating and incorporating the Government's data confidentiality requirements into an SLA, there remains much ground to cover in regards to the development of the concept of assurance and trustworthiness when government agencies procure external information system services from services providers.

Further, although the concept of security-related SLAs has been studied for a while [31–38], there has been a gap in the investigation of how to incorporate data confidentiality considerations into an SLA between the Government and its service providers. The usefulness of this insight would provide a greater understanding of providing SLA-based discrete levels of security assurance that include the protection of sensitive government data based on the data classification and risk level. This, in turn, can be used to help inform the idea of proposing a TDSLA capability framework as a means of incorporating data security requirements (considering the Government's data confidentiality requirements) into the formulation of SLA-based discrete levels of security assurance. This is in line with one article of provisions of the Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012.

In essence, the main research question addressed in this thesis was: **How can the Indonesian Government's data confidentiality requirements be incorporated into a service level agreement?**

The purpose of the research in this thesis has been directed into three qualitative studies that incorporate views from representatives of the Government and service provider experts. The first qualitative study has investigated the Indonesian Government's security needs to mitigate unauthorised access to sensitive government data in response to the problem of preserving the confidentiality of government data after the secret documents made public by Edward Snowden. The first study reports on the importance of having information security agreements when using such external services. The second study has examined the perceptions of government SLA data confidentiality requirements using 35 participants (government employees and government consultants) using GADM. The third qualitative study has attempted to explore the current provisions of SLAs provided by service providers to Indonesian government agencies and identify possible service provisions for data confidentiality in SLA contexts. As such, this study conducted a longitudinal study of the Government auctions of 59 e-procurement services across 80 Indonesian government agencies between 2010 and 2016 to select major service providers that provided Internet services, cloud-based services and data centre services. Five selected service providers were then contacted to participate in another GADM with 15 participants.

The work on the Indonesian Government's data confidentiality requirements is a guide to develop principles for a TDSLA capability framework. As such, a grounded theory analysis was employed to examine the Delphi study data from the two previous qualitative studies (Chapter 5 and Chapter 6). Such analysis aimed to identify concepts and categories which turned into principles, thus providing a framework for building a trustworthy data security level agreement capability. The principles and framework that emerged from the data were evaluated and validated using three approaches, namely: 1) reflection against related work; 2) application of transferability through two real-world cases from Amazon Web Services (AWS)-the UK Government Cloud and the US FedRAMP; and 3) testimonial validity through participants' feedback.

8.2 Contributions

8.2.1 Methodological Contributions

The essential contribution that has emerged from investigating Government's data confidentiality requirements is a method that addresses the specific limitations of engaging with senior officials from Government and the private sector all of whom have security postures to protect. Described as an adaptive Wideband Delphi method this approach is based on elements of the traditional Delphi method and Wideband Delphi method. This method is a practical way of eliciting Government's security needs by using specific Delphi features, such as anonymous individual feedback, controlled feedback and group responses with face-to-face meetings (described in Chapters 3 and 4).

An additional methodological contribution made in this thesis has been the application of grounded theory to the transcripts of the Delphi study data as a means of providing greater theoretical understanding (described in Chapters 3, 5 and 6), as shown in Figure 8.1. Combining these two approaches allows the researcher to gain additional validity from the results as both methodologies complement each other. An adaptive Delphi method is useful in obtaining a genuine understanding of the issues and the validity of the research through an iterative process and respondent validation. A grounded theory provides a robust

qualitative analysis to examine the Delphi study data in more detailed categories, thereby gaining a more robust understanding that can be used to develop theoretical insights and practical recommendations.

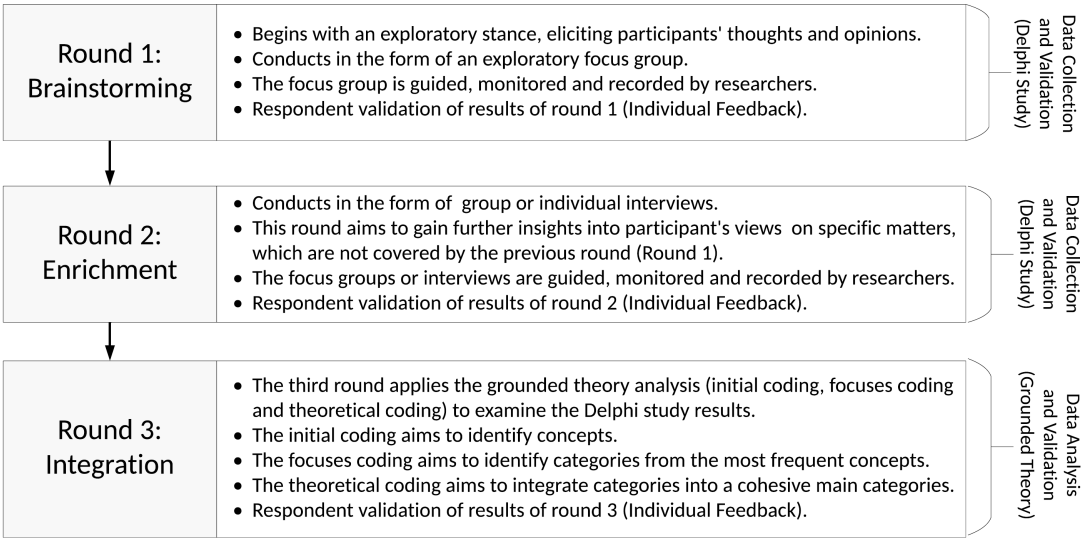


Figure 8.1: Proposed a Grounded Adaptive Delphi Method (GADM)

8.2.2 Empirical Contributions

This thesis also makes its contributions on the basis of the three studies, explained in Chapter 4, 5 and 6 respectively, that describe: perceptions of government security needs; SLA data confidentiality requirements; and service provision for data confidentiality in SLAs.

The findings outlined in Chapter 4 identify 25 categories of government security needs which are framed by the five primary elements: people, operations, technology, governance and legal remedies. Some categories of government security needs are in line with the existing security controls, such as ISO/IEC 27002 and NIST 800-53 while some security needs appear novel to the Government in their efforts to mitigate unauthorised access to sensitive government data.

The findings described in Chapter 5 uncover three perceptions of incorporating the SLA data confidentiality requirements into an SLA. The first perception introduces 21 concepts within three main categories of target of protection, namely: 1) human asset; 2) information

asset; and 3) physical asset. The second perception presents 17 concepts within five main categories of risk perception, which are: 1) collaborator; 2) exfiltration; 3) observation; 4) insertion; and 5) manipulation. The third perception introduces 22 concepts within five main categories of government SLA data confidentiality requirements, namely: 1) access management; 2) data management; 3) identity management; 4) malicious management; and 5) compliance management. The findings can be used to guide the development of a TDSLA capability framework as a means of incorporating the Government's data confidentiality requirements in the formulation of SLA-based discrete security assurance levels.

The findings described in Chapter 6 identify three central themes that have emerged in the empirical study: 1) risk perception; 2) current provisions of SLAs; and 3) possible service provisions for data confidentiality in SLAs. The findings of the study have identified ten concepts of risk perception within five categories of security concerns. The majority of concepts identified are in line with the categories of risk perception identified in Chapter 5, except one category regarding the denial of access, which is not one of the confidentiality considerations. Furthermore, the findings have identified six concepts within four main categories of current provisions of SLAs, namely: 1) availability; 2) response time; 3) resolution time; and 4) other. The findings also have identified and described 17 concepts within four categories of service provisions for confidentiality, namely: 1) technical provisions; 2) physical provisions; 3) procedural provisions; and 4) human provisions. Such provisions for data confidentiality can be considered for inclusion in SLA contexts.

8.2.3 Conceptual Contributions

Other contributions of this thesis are developing foundations for a TDSLA capability framework and validating the emerged principles and framework using three approaches. The approaches are namely: 1) reflection against related work; 2) testimonial validity through participants' feedback; and 3) application of transferability through two real-world cases from Amazon Web Services (AWS)-UK Government Cloud and US FedRAMP.

The resulting principles and framework developed were based on the Delphi study data. By employing the grounded theory analysis, this thesis has presented five principles as the

building blocks of the proposed framework. Another contribution is a critical review of the latest thinking of providing security-related SLAs as described in Chapter 2, specifically as it applies to incorporate data confidentiality considerations into an SLA.

8.3 Discussion

Based on the findings of the grounded adaptive Delphi studies, principles for building a TDSLA capability framework have been developed to facilitate the incorporation of Government's data confidentiality requirements into an SLA. One benefit of using such a framework is that the ability of the framework to include not only existing security controls but also discrete security assurance levels based the data classification and threat model. This framework has allowed service providers to deliver the required data confidentiality capabilities that, at a minimum, meet the technical requirements for the required level of security assurance.

The framework leads to a simple means of incorporating the Government's data confidentiality requirements into an SLA between government agencies and service providers. In other words, it allows government agencies that do not have the technical knowledge to specify government security needs. For example, a government tender could entail security assurance level 3 (SAL3) for processing biometrics data while service providers that are keen to provide such services are required to satisfy the required level of assurance.

An essential decision in the formulation and classification of the Government's data confidentiality requirements into discrete security assurance levels was the need to ensure the simplicity and clarity of the TDSLA capability framework. The aim is to provide sufficient practical knowledge to novice staff without requiring them to learn how to classify data confidentiality requirements and capabilities according to data classification and threat environment. Additionally, a government tender can evaluate whether or not the service provider has demonstrated a set of security requirements specified in the required level of security assurance.

Further, government agencies that possess deficiencies in identifying the required confidentiality capabilities can select an appropriate service provider that provides the level of

security assurance required to protect sensitive data, thereby improving the overall quality of government procurement of external information system services. An approach for expressing security assurance levels in the form of SLAs has received paramount attention from the Government and service providers as practical means of assuring service scenarios. Discrete levels of security assurance are essential in defining a TDSLA capability framework.

In answer to the primary research question, 'How can the Indonesian Government's data confidentiality requirements be incorporated into a service level agreement?'— the principles and framework that emerged from the Delphi study data are useful and practical contributions to address such a question. From the main research question, three sub-questions are derived to conduct more detailed studies of the research topic. The first sub-question SQ1 aims to study government security needs to mitigate unauthorised access to sensitive government data. The question SQ2 seeks to investigate government SLA data confidentiality requirements. The third question SQ3 examines the current provisions of SLAs and identifies possible service provisions for data confidentiality. Finally, in order to address the central question of this thesis, Chapter 7 presents principles as foundations for a TDSLA capability framework through a qualitative analysis of the two previous studies (described in Chapter 5 and Chapter 6). In answer to those questions, qualitative research using an adaptive Delphi method, grounded theory and the GADM approach constitute appropriate approaches.

From a methodological point of view, developing an adaptive Wideband Delphi method provides a useful means of exploring and eliciting original participants' opinions and ideas regarding the sub-research questions as well as overcoming the problem of conducting real-world qualitative data collection activities with elite participants such as government officials. This approach provides a flexible and systematic means of collecting detailed information while maintaining validity in the research process by minimising bias and maximising transparency. Such an approach can also offer insights into a wider range of similar settings. It is note that a great effort was made to conduct the meetings during the Delphi studies, especially to be able to interact with time-constrained elite participants. Although the method used in this thesis is labour-intensive and expensive, it is a practical way of investigating the Government's confidentiality considerations by using specific

Delphi features, such as anonymous individual feedback, controlled feedback and group responses with face-to-face meetings [14].

It is noted that the adaptive Delphi method aims to exploit the different views, opinions, thoughts, and experiences of individual participants on specific matters, with greater generalisability across various participants. Therefore, combining the adaptive Delphi method with a detailed grounded theory analysis provides a rigorous approach to solving complex real-world problems. Further, the grounded theory analysis is particularly well-suited for capturing such different views from participants. In this case, the Delphi method aims to distil the judgement and statements of participants through successive iterations of group discussion and individual feedback, whereas grounded theory is an approach to identifying ways of understanding participants' ideas and opinions. In other words, the grounded theory analysis is used to support Delphi study results to create a theory for the development of principles and framework.

From a substantive point of views, the grounded theory analysis provides a useful theoretical framework for examining the Delphi study data. In some Delphi studies, it aims to reach a consensus in a body of knowledge [179]. However, getting stakeholders to reach consensus on a final decision can be extremely difficult, and it takes time and effort to build consensus across participants. The objective of the Delphi method in this thesis is not to achieve consensus but to explore diverse ideas, opinions, and views regarding a specific question. Thus, the grounded theory analysis attempts to replace a consensus view with the judgement of a few participants by conducting initial coding, focused coding, theoretical coding [108], and transferring understanding into a set of principles as building foundations for a TDSLA capability framework.

The methodology used in this thesis can be useful for future research as a means of investigating other government scenarios. When conducting the approach to government settings, it is necessary to ensure that participants have a clear understanding of the problem description and the Delphi steps before the study begins. This assumes that participants are given sufficient time to consider the importance of the research objectives and researchers are well-connected with participants to ask their participation in several Delphi rounds.

8.4 Limitations

There are a few challenges in the application of the concept of a TDSLA capability framework. One of the main concerns about the framework is its applicability in the real world and the need for further elaboration using a wider range of information system services. Further work is required to examine acceptable discrete levels of security assurance in different service provisioning scenarios and to consider how the TDSLA framework would apply to each of these scenarios.

There are two main questions for which the concept of a TDSLA capability framework may be applied in various service scenarios. Firstly, how to incorporate discrete security assurance levels into the context of SLA would need to be expressed. Secondly, how to evaluate whether the use of discrete security assurance levels required is in line with customer's requirements and service provider's capabilities. The means of compliance checking is not worth much attention until clear definitions of discrete levels of security assurance are provided. As such, it is necessary to formulate and classify distinct technical requirements for each security assurance level.

Another challenge is in characterising data confidentiality risks within each discrete security assurance level, especially when attempting to include specific risks or threat model into SLA contexts. Such threats are guaranteed to be mitigated based on the discrete level of security assurance required. For example, in the case of purchasing insurance, the degree of exposure to a particular type of risks or threats can be predicted and guaranteed with pricing levels [31]. However, in the case of assurance services, it is hard to estimate the costs of maintaining security capabilities, as security risks or threats identified for each discrete level of security assurance tend to behave unpredictably from time to time.

Further, an additional difficulty is how to classify data confidentiality capabilities according to threats, especially when government agencies decide to procure external information system services to process, store, or transmit sensitive data on behalf of the Government. For instance, SLAs can be formulated based on specific levels of threats and technical requirements to sensitive government data. However, it is difficult to require explicit assumptions about the service provider's capabilities to be included in the form of SLAs. Also, there is a

risk of liability and compensation with the incorporation of appropriate discrete levels of security assurance into SLA contexts. These questions have been identified as future work.

A final criticism can be directed to the methodology used in the research including research design, setting and participant, data collection technique and data analysis. Despite the measures taken to validate and generalise findings, the ability to make generalisations based on this study is limited by the number of participants from a single country. Additional cases with more participants from other countries might present more fundamental principles, with more capacity for generalisation. Overall, these limitations provide opportunities for future research to build on the findings of this study.

8.5 Reflections on the Research Process

8.5.1 Reflection on data collection experiences

Several challenges arose during data collection activities. Firstly, the author of this thesis experienced data collection challenges related to the researcher himself. Although the researcher is an Indonesian civil servant, the researcher had some difficulty establishing rapport with participants. The researcher also faced challenges on how to convince them to participate, especially when dealing with sensitive topics, and encountering participants who were uncomfortable speaking to and sharing confidential information with the researcher.

Furthermore, the researcher, at times, did not feel confident in conducting qualitative research with government entities, service providers, and other related parties because the research undertaken was labour-intensive and time-consuming, requiring support from the Government for data collection activities. For example, this study began with submitting a research proposal to the Directorate of Information Security, the Ministry of Communications and Informatics. After receiving confirmation and approval from an official, all participants received an official invitation letter to participate in the study.

Secondly, participants' perceptions of data collection activities were also identified. Majority of participants had concerns about the confidentiality of their opinions and statements. As such, participants were reassured of the secrecy of their views by ensuring that their responses were made anonymous by de-identifying data. Sometimes, participants

felt uncomfortable when they were revealing sensitive information to the researcher. They usually did not explicitly describe such information in detail. Moreover, in a minority of cases, participants did not read the questions before attending the meeting, and the answers to such questions were very spontaneous based on their experience. However, it was useful to obtain genuine opinions from participants.

Thirdly, the researcher faced challenges related to the venue of focus groups for the Delphi data collection. The researcher requested access to a meeting room to avoid the cost of hiring the place. In some cases, the researcher anticipated beforehand if any participant did not attend the meetings by providing access to video conferencing and group video calls. The most important consideration was related to logistics issues. Fortunately, all data collection activities were supported by the Government of Indonesia.

Fourth, data collection challenges experienced while conducting the research design through several empirical studies. The researcher faced difficulties in maintaining participant responses. During the first round of Delphi, it was a difficult stage for the researcher to gather all participants in one location to perform a kick-off meeting and brainstorming session. Although the researcher successfully invited all participants to attend a kick-off meeting during the first round of Delphi as presented in Chapter 4, it was a good practice to perform brainstorming session in separate groups (comprising of participants from similar expertise), as shown in Chapter 5 and Chapter 6. In this round, participants who were not able to attend face to face meetings could participate through video conferencing.

Another challenge faced by the researcher was not all participants could participate in all meetings (all Delphi rounds). However, the researcher sent results or transcripts for each round to all participants to receive their feedback. It was clear that maintaining participants in the Delphi studies was difficult. It is note that not all participants responded to all questions and gave individual feedback for incorrect responses or interpretations.

In short, such data collection activities may likely represent a challenge for other researchers, who do not have good contacts with elite government experts, to generate the same results, using the same research methods with a similar setting and participants. In other words, only specific researchers could carry out such research successfully. Otherwise this would be highly unlikely to happen if such activities were related to sensitive matters.

8.5.2 Reflection on data analysis experiences

The original idea of the Delphi method was to obtain a consensus of participant opinion on an emerging issue through a series of Delphi rounds. However, not all Delphi studies aim to achieve consensus, such as the Delphi method used in this study. As presented in Chapter 4, during the third round of Delphi, the researcher conducted a consolidated meeting instead of a consensus meeting. The researcher combined various categories of government security needs from different groups into a set of categories of government security needs. For other Delphi studies, the researcher conducted a grounded theory analysis of the Delphi study data by conducting initial coding, focused coding, theoretical coding [108] to replace a consensus or consolidated meeting, as it was expensive and difficult to hold such a meeting.

Furthermore, the researcher conducted the Delphi method to identify diverse opinions on specific questions as the part of the individual and group responses, whereas the grounded theory approach aims to develop a new theory or a framework from the Delphi study data. The researcher did not use grounded theory as a method because of its time-consuming nature. However, the researcher borrowed its coding technique comprising of three cycles of coding (initial coding, focused coding, and theoretical coding) to examine the Delphi study data to identify concepts and categories which were compiled to derive principles as foundations for a TDSLA capability framework.

The researcher started initial coding by using the participants' statements to minimise the possibility of subjectivity [108]. The researcher experienced difficulties in understanding how to conduct the three levels of coding and subsequent theory development. As such, the researcher applied constant comparison to identify patterns and similarities within and between different transcripts. The researcher also created a spreadsheet that indicates the relationships between each level of coding as well as their connection to theory development.

In conclusion, as a beginner grounded theorist, the researcher initially faced difficulty in data analysis. It took a while to develop an understanding of grounded theory to undertake this study. The researcher took several backwards steps during analysis, and such codes, concepts and categories were repeatedly corrected to conclude the report.

8.6 Directions for Future Work

While this thesis has demonstrated the potential of incorporating the Government's data confidentiality requirements into SLA-based discrete security assurance levels, many opportunities for extending the scope of this thesis remain. This section presents some of these directions.

8.6.1 Developing government data classification for cloud readiness

Data classification schemes have been used for decades to help governments improve the protection of sensitive data and manage the confidentiality and integrity of government data. Every government has different terminology models that define the classification of government data including the levels of risk and sensitivity. In other words, it is necessary to acknowledge various types of data handling and management constraints over the data (e.g. data protection, national security, and health regulations).

The definition of sensitive data differs amongst government agencies; for example, each government agency has various types of sensitive data, such as health or medical information, financial data, military and defence data, law enforcement data, and citizen data. Therefore, the Government should develop a data classification scheme that provides the guideline for determining the appropriate level of protection within government agencies. Thus, the classification of data should consider along the lines of data that is critical to national security, personal data, sensitive business data and publicly available data.

In the context of Indonesia, according to Article 17 of the Indonesian Law on Public Transparency Number 14 of 2008, the Government defines three categories of data classification: 1) public; 2) restricted; and 3) secret. Public information could be shared and accessed by many entities. Restricted information is subject to legal restrictions which could be shared upon request with other entities for official purposes. Secret information could not be shared with those individuals who do not have a legitimate reason for needing the information. The provisions of the law do not provide detailed security requirements and level of protection for each data classification. In addition, the Government Regulation Number 1 of 2017 on a classification of government data as the elaboration of the Indonesian

Law Number 14 of 2008 does not give more detailed security requirements for inclusion in each data classification.

Further, according to the National Archive Regulation Number 17 of 2011 concerning Government Security Classifications and Archives, the Government outlines four categories of government security classification both physical and electronic documents, namely: 1) public; 2) restricted; 3) secret; and 4) top secret. Although the regulation outlines what is required for each level of classification, it is unclear how such requirements will be enforced. There is no technical detail concerning the security requirements for each category.

Another challenge comes from the Government Regulation Number 82 of 2012. The Government requires service providers (including cloud service providers) that handle data related public services, such as medical records or citizen data are needed to store such data in Indonesia. As presented in Chapter 5, there is an absence of government data classifications applied to government agencies that generate, process, collect, store and transmit classified and sensitive data.

One possible direction of research is to elaborate more on classifying government data as presented in Chapter 5. The existing laws and government regulations do not give detailed security requirements for inclusion in each data classification, as there are downsides to encoding detailed security requirements in law and government regulation (such as if the law becomes too prescriptive, it more easily becomes too limited and obsolete). In the context of Indonesia, the Law and the Government Regulation mandate the Government to establish a ministerial regulation that explains technical provisions of the laws and regulations. The encoding detailed security requirements in a ministerial regulation is taken from related law and government regulation as a legal basis and guidelines for government security classifications. The ministerial regulation can be revised to reflect changed circumstances.

Therefore, it is worthwhile to investigate a framework for the Government security classification, as the existing laws and government regulations do not provide detailed the Government's security requirements for each data classification. In doing so, any external information system services that process, transmit and store sensitive government data have to preserve the confidentiality, integrity and availability of the data. Further, it is worth noting such a data classification scheme can yield significant benefits to procuring

cloud-based services from cloud service providers. Adapting the UK Government Security Classifications [89] in the context of Indonesia would be useful to consider for future research. Future work needs to consider the additional empirical work necessary to develop a government data classification scheme for cloud readiness. In so doing, the possibility of implementing *Principle 1* becomes conceivable.

8.6.2 Developing confidentiality threat models

Developing threat models is labour-intensive work requiring people with specific security experts, who know how attacks work. The formulation of five categories of confidentiality risks presented in Chapter 5 can be extended in several ways. One possible extension is to classify threat models for each discrete level of security assurance. As described in Chapter 5, the five categories of confidentiality risks, namely: 1) collaborator; 2) exfiltration; 3) observation; 4) insertion; and 5) manipulation. However, schemes for classifying such threat models into security classifications are not straightforward. It is expected that the discrete levels of security assurance protect against increasing scale and sophistication of threats - for example - government data classified at one level cannot be assured to be protected against threat models described in a higher level of assurance.

Another possible extension is to enrich the expressiveness of threat model statements. Without an actual threat model, it is difficult to classify a threat to a particular level of security assurance. More recent works have modelled the different categories of confidentiality threat models [53, 180]. These examples of related work in the area have highlighted the need for a generalised and well-formalised threat model. It should be possible to go one stage further to capture all types of confidentiality threats in a distinct manner using the GADM approach. People with specific expertise who know attacks play out will be required to participate in future work. It is expected to develop a catalogue of generic threat models from empirical data. The proposed threat models for each level of security assurance should be general so that it can be applied to various services. Thus, it is worthwhile to investigate a set of threat models for each discrete level of security assurance. In so doing, the possibility of implementing *Principle 2* becomes feasible.

8.6.3 Developing government SLA data security requirements

As reported in Chapter 5, the initial formalisation of government SLA data confidentiality requirements is introduced. Standardisation of such provisions is an essential direction for future research. Some of the previous works [47, 59, 60, 62] to the development of government security requirements have been described in Chapter 5.

As far as we are concerned, there is only one approach that is more suited to develop government data confidentiality requirements. Although such security requirements presented in NIST SP 800-171 are mainly concerned with the protection of the confidentiality of controlled unclassified information when using external information system services from external service providers, the confidentiality requirements are not directly applicable to SLAs in general. Such confidentiality requirements are derived from existing security controls such as NIST SP 800-53. This thesis and future work aim to increase the consideration of the Government's data confidentiality requirements in SLA definition when using external information system services from service providers.

One interesting question is whether the definition of government SLA data confidentiality requirements can be developed from qualitative studies. If this is the case, selecting appropriate participants for future research will have an impact on data collected. Therefore, it is paramount to select participants based on the diversity of experience and expertise. As presented in Chapter 5, this thesis has introduced five categories of government SLA data confidentiality requirements employing 35 participants (government employees and government consultants) based in Indonesia using a grounded adaptive Delphi study [13].

Thus future work needs to elaborate such requirements into a general SLA data security requirements. This is best accomplished through engagement with a group of participants from each government agency across a total of 80 Indonesian government agencies. The applicability of GADM should be considered in this respect.

8.6.4 Developing discrete security assurance levels

The findings of this study indicate that discrete levels of security assurance play an essential role in supporting the definition and inclusion of the Government's data confidentiality

requirements into an SLA. The discrete security assurance levels presented are evidently in need of further elaboration. This is best accomplished through engagement with government, industry and other relevant stakeholders. Participants will be asked to identify the technical requirements for four discrete levels of security assurance. As described in Chapter 7, each security assurance level consists of confidentiality considerations of Principle 1, Principle 2, Principle 3 and Principle 4. Thus, data confidentiality considerations presented at each level developed based on the statements from the participants of this study.

Therefore, further work needs to elaborate such requirements more clear by adapting approaches from NIST SP 800-63 that defines four levels of assurance for authentication and FIPS 140-2 that defines four levels of security for cryptographic modules [74, 75] and applying to various service scenarios. It is expected that the discrete levels of security assurance can be adjusted to cope with the increasing sophistication of the threat environment. It is anticipated that each discrete level of security assurance offers an increase in the range of threats addressed over the previous level. These four increasing levels of security assurance allow cost-effective solutions that are appropriate for various applications and domains.

8.7 Conclusion

The research reported on in this thesis has investigated a future assurance approach for service provisioning based on discrete levels of security assurance incorporated into SLA contexts. The work on the Indonesian Government's data confidentiality requirements was used to develop foundations for a TDSLA capability framework. This resulted in an initial TDSLA capability framework. However, it is anticipated that the concept of a TDSLA capability framework can be broader to other data security requirements. In other words, four discrete levels of security assurance can be extended and elaborate on other security properties of data integrity and data availability.

The key inspiration and reference point for building a TDSLA capability framework is the CC certification process. CC aids to build trust through two main components, namely: protection profiles; and evaluation assurance levels (EALs). Whereas, developing foundations for a TDSLA capability framework consists of two main parts, namely: discrete security assurance levels; and service level agreements.

A discrete level of security assurance defines a standard set of data security requirements for a specific type of threats and data classification level. The technical, procedural and human elements of information security are necessary to achieve the required level of security assurance. Each level of assurance is distinct from another, depending on data classification and threat model. In addition to discrete security assurance levels, the use of service level agreements is intended to examine the service provider's capabilities to meet the customer's data security requirements and to agree with the required and provided level of security assurance among contracting parties.

Therefore, these are the reasons to construct better assurance mechanisms in service provision that give government agencies as much transparency and confidence as possible that any sensitive government data transferred to service providers is processed, transmitted and stored securely against unauthorised access. In other words, the CC aims to certify levels of security for products while the TDSLA capability framework aims to certify levels of security for services.

This study was the first of its kind in Indonesia to take a holistic assurance approach to service provisioning in government procurement by engaging all three types of entities, namely permanent government officials, government consultants and service providers. It has provided a much-needed evidence base to support the more widespread implementation of the TDSLA capability framework. In doing so, this thesis makes a significant contribution to service provision, with a focus on the Indonesian Government. Finally, this research endeavour hopes to pave the way for further investigations of better security assurance for services in global computing environments.

Appendix A

Grounded Theory Analysis

This appendix contains documents relevant to the grounded theory analysis reported in this thesis. Given the large volume of data generated, elements of the TDSLA capability framework are shown as a representative sample of the overall analysis. Each of the following tables shows a sample Delphi study transcript together with associated concepts and category.

Data/incident (Translation)	Concept	Category
if the person is a senior official who carries out government duties, such person is subjected to be protected all the time because it is considered as an asset	protecting government officials	Human Assets
the secrets belong to government officials, such as a president can be uncovered by examining his/her previous unprotected information	protecting government officials	
The most sensitive information is stuck in the heads of senior officials	protecting knowledge and experience	
Public information that if opened may subject to the protection of intellectual property rights and the protection of unfair competition data	protecting intellectual property	
every government agency is required to define sensitive data in their terms because the type of sensitive data in each agency differs with other agencies. For example military and defence data	protecting military and defence data	Information Assets
in some cases, the distinction between sensitive data and non-sensitive data looks “grey”, for example, one has uploaded the entire government meetings including their internal meetings to social media, such as Youtube, with the aim to build trust to the public. However, some of the information should not be disclosed for public consumption, such as personal data and privacy	protecting personal data and privacy	
Related to protecting public sector data, there is currently a term called health security, which deals with the protection of health data	protecting health or medical records	
It is necessary to ensure adequate physical protection for information system facilities and infrastructures, such as data centre, networks, systems and devices	protecting information systems	Physical Assets
the need for protection of critical national infrastructure that has huge impacts on the human society, such as electricity and health facilities	protecting critical national infrastructure	
the components that need to be protected relate to aspects of public and government services	protecting government services	

Data/incident (Translation)	Concept	Category
if we look at the present state, almost all cases of data leaks occur because of an insider, whether committed by an employee or a former employee	identifying insider threats by employees	collaborator
the issue of sensitive government data theft normally does not occur while data is transmitted, but when data was processed or created. While having a discussion with...an insider can listen and participate in the discussions and then disclose and share the information obtained with an adversary	identifying insider threats by employees	
service providers have a better understanding of how to gain access to resources, such as data centres that store confidential data	identifying insider threats by service providers	
There is a threat, which we consider before the threat was always from the outside, so we then place a firewall, intrusion detection, and so forth. But the fact that now the threats and attacks actually come from inside...according to our observation, we discovered botnets keep sending out information	Identifying outbound traffic	exfiltration
service provider should provide explicit guarantees regarding the security of the data it manages. How the service provider secures the data, as required should be explained to the customer. Then, the need for a monitoring system to ensure that the data is not transferred or copied to unauthorised parties	identifying content exfiltration by a service provider	
when we communicate, we must remain aware of our level of communications, whether or not it is important in relation to confidentiality of information transmitted...we are aware that when we are talking with our interlocutor, there must be other people listening without knowing them	identifying interception (content/traffic)	observation
the most in need of government secrets is foreign intelligence agencies. They need such information for their purposes	identifying discovery by foreign government	
they embed code on the opposing side in any way to divulge the sensitive government data	identifying a malware injection	insertion
An example of a case that it occurred in one agency which administers the national health insurance, which was attacked by malware where all the data on the server was encrypted	identifying a ransomware installation	
For threats to military information and sensitive government data, in general the threats were in the form of impersonation. Besides the impersonation, they can also do phishing	identifying impersonation attacks	manipulation
Email and web are such vectors for delivering phishing attacks because both vectors are frequently accessed via mobile and desktop	identifying phishing attacks	

Data/incident (Translation)	Concept	Category
we should require every employee in government agencies to have a public key and a secret key when communicating through government email services because the content of email communications and its metadata needs to be protected	requiring secure communications	access management
It is important to allow who is entitled to access the data. However, authentication is required to enter the systems	requiring access control to sensitive data	
As an example, the secret communications between the Ambassador and the Ministry of Foreign Affairs. The line of communication has been secured using secure channels. When both parties receive information, the information is stored in a secure storage facility. However, when the process of making such information there is no way to protect the data during processing	requiring encrypting data during processing	data management
The need for security requirements to protect sensitive government data based on the level of confidentiality, including restricted, secrets and top secrets so that appropriate controls can be implemented to protect government data at each classification	requiring adequate data classification controls	
To access government secrets-information of interest to nation states, it requires a combination of four of the seven senior government employees who hold passwords to access such sensitive information	requiring multi-factor authentication	identity management
such access will be provided by needs and job descriptions so that such person can not access all government information systems	requiring privileges to access sensitive data	
it seems that security controls should be integrated with physical elements, such as a room, doors and locks that need to be installed	requiring physical security	malicious management
Security screening and access control list should exist. Such access restriction is implemented based on a need-to-know basis	requiring appropriate personnel security screening	
The business process applied constantly considers the security aspect of preserving the confidentiality of sensitive data, and they must ensure that all business processes are compliant with security standards and best practices	requiring compliance with standards and regulations	trust and compliance management
By applicable regulations, electronic system operators, who handle public sectors, are divided into three categories of impact namely Low, High, and Critical. Both high and critical categories are required to have ISO/IEC 27001 certification with additional controls for a critical category	requiring certification and attestation of suppliers	

Data/incident (Translation)	Concept	Category
In the context of cloud computing, the required security requirements are mostly related to the connectivity with virtual private networks	providing secure connections	technical security provision
For data in motion, we can do encryption, using SSL, IPSec or VPN. For data at rest, we can make use of data encryption and data loss prevention, and for more advanced technologies for cloud customers, we can provide storage encryption or hardware security module	providing encryption	
When the data is encrypted, the key must be held by the custoner not the provider	providing key management	
To mitigate risks related to malware and viruses, we have anticipated by checking our devices	providing malware protection	
we guarantee the availability of CCTV devices, door access and visitor access management	providing CCTV, providing visitor access	physical security provision
To enter the data centre, there are controls in place to prevent misuse. Also, there is a log book, and the server is caged and locked at a standard facility	providing security cages	
Usually the security required for colocation services is physical security. what kind of control is required to enter the data centre	providing access cards	
Vulnerability assessment and penetration testing services can be provided to customers if needed	providing vulnerability assessment	procedural security provision
We should comply with ISO 27001 because there already has service delivery, service agreement, third party agreement, assurance, cryptography and so on. It should be enough for us to define confidentiality requirements in SLAs. The standard covers not only technology but also covers people and process	providing compliance with standards	
For example, government as a customer already have user access matrix. So the access control can be adjusted with applicable user access matrix and policy from a customer side	providing use access matrix	
If we consider security, we not only look at from the technology side, but we must know how the process and procedure. Personnel should be well-educated or know what to do. Once he has access rights, it must be managed properly	providing security training	human security provision
We have to protect sensitive data from insider threats	providing personnel security	
The concept of security is widely discussed. Generally we discuss in terms of technology. Though there are still people and processes. For example, how to handle complaint handling	providing security training	

The following list details all the codes that were generated in this study.

Code

Protecting banking information
Protecting business sensitive data
Protecting citizen data
Protecting communication channel
Protecting confidential diplomatic communications
Protecting credit card information
Protecting critical information assets
Protecting critical information infrastructure
Protecting critical national infrastructure
Protecting customer data
Protecting data intelligence
Protecting data procurement
Protecting defence and military data
Protecting defence and national security data
Protecting demographic information
Protecting devices
Protecting ecommerce data
Protecting education data and research data
Protecting election and political data
Protecting email communications
Protecting employee data
Protecting exchange rate against currencies
Protecting financial information
Protecting government and military data
Protecting government budget
Protecting government communications
Protecting government secrets, including military and defence data
Protecting government services
Protecting health information
Protecting health or medical records
Protecting identity number and driving license
Protecting information systems
Protecting intellectual property
Protecting intelligence data
Protecting intelligence data and national security data
Protecting knowledge and experiences
Protecting law enforcement data
Protecting medical data/information
Protecting medical records about senior government official
Protecting metadata (log files)
Protecting metadata of a file or communications

Protecting metadata of email communications
Protecting military and defence data
Protecting mining, oil, gas, natural resource databases
Protecting national budget, government budget, military budget
Protecting national crypto information
Protecting national defence and security
Protecting national economic and interests
Protecting national health information
Protecting national identity
Protecting national security data and economic sensitive data
Protecting natural and energy resources data
Protecting official communications
Protecting official communications via email
Protecting passport and biometric information
Protecting password
Protecting patient and pension data
Protecting patient data and medical records
Protecting payroll data and systems
Protecting personal data and privacy
Protecting political data and national security data
Protecting political information and senior government officials
Protecting president as a national asset
Protecting procurement tenders
Protecting public, official, secret data and top secret
Protecting senior government officials
Protecting sensitive data against corporate espionage
Protecting sensitive data against data theft
Protecting sensitive data against insider threat
Protecting sensitive data in a physical form
Protecting sensitive economic data and disaster database
Protecting sensitive economic figures
Protecting sensitive information from combined attacks
Protecting sensitive information from unauthorised portable storage
Protecting sensitive information with cyber insurance
Protecting stock exchange
Protecting tax information
Protecting unsecure infrastructure
Protecting untrusted channel
Protecting untrusted cloud provider
Protecting untrusted communications and devices
Identifying a malware injection (trojan/backdoor)
Identifying a malware injection and untrusted website
Identifying a man in the middle attack
Identifying a ransomware installation
Identifying a well-funded state actor

Identifying anomaly attacks
Identifying application vulnerabilities to access data
Identifying APT attacks and state sponsored attacks
Identifying auction for stolen sensitive information
Identifying audit attacks
Identifying authorised access to data
Identifying authorised software and hardware
Identifying backdoor to access data
Identifying backdoor using audit
Identifying backdoor using embedded code audit
Identifying browser exploits
Identifying brute force attacks to access data
Identifying cloning attack
Identifying compromised certificate authorities
Identifying compromised credential information
Identifying compromised encryption
Identifying connected devices to access data
Identifying content exfiltration by a service provider
Identifying credit card abuse
Identifying cross-site scripting attacks
Identifying data auction by hackers
Identifying data disclosure
Identifying data exfiltration by connected devices
Identifying data exfiltration by emails and virus
Identifying data exfiltration by malware
Identifying data interruption
Identifying data leakage (e.g. on USB Port)
Identifying data modification
Identifying DDoS attacks
Identifying deniability
Identifying discovery by foreign governments
Identifying disgruntled employee and insiders
Identifying eavesdropping and man in the middle attack
Identifying embedded backdoor router devices
Identifying embedded malicious code
Identifying endpoint vulnerabilities
Identifying external service providers
Identifying fake certificate
Identifying hackers to auction sensitive data they stole from governments
Identifying hacking by order and using auction
Identifying human and technology elements
Identifying human as an attack surface
Identifying human factors like insiders
Identifying illegal access and gathering credential such as PIN
Identifying impersonation attacks

Identifying social engineering, malicious code, hacking
Identifying social engineering
Identifying software with backdoor
Identifying SQL injection
Identifying state actors to access sensitive data
Identifying supply chain attacks
Identifying system failure
Identifying technical and non-technical attacks
Identifying the disclosure of sensitive national security information
Identifying the sabotage of sensitive data and services
Identifying the weakest link to access data
Identifying threat actors (organised crime, APT)
Identifying threat profiling and DDoS attacks
Identifying transmission attacks
Identifying unauthorised access (people)
Identifying unauthorised access (using vulnerabilities)
Identifying unauthorised actors
Identifying unauthorised applications installed
Identifying unauthorised data disclosure (people)
Identifying unauthorised data transfer
Identifying unsecure and trusted external providers
Identifying untrusted providers or uncertified providers
Identifying untrusted website
Identifying USB as an attack vector
Identifying user anonymity
Identifying VM Vulnerabilities
Identifying vulnerabilities to access data
Identifying vulnerabilities to hack databases
Identifying web app attacks and social engineering
Identifying web deface, scanning and data interruption
Identifying zero day attacks to conduct unauthorised access
Identifying zero day vulnerabilities
Identifying zero days attacks to access data
Identifying zero days vulnerabilities
Requiring a remote access through VPN
Requiring a strong regulation
Requiring a zero access mechanism to sensitive data
Requiring access control and security protocol
Requiring access control to sensitive data and privileges
Requiring accountability
Requiring adequate data classification controls
Requiring air-gapping and isolation
Requiring antivirus services
Requiring appropriate personnel security screening
Requiring architecture policy

Requiring assurance and standard
Requiring assurance for provider's security capabilities
Requiring assurance using code review
Requiring assurance using common criteria
Requiring assurance using source code analysis
Requiring audit compliance and monitoring
Requiring audit trail
Requiring auto-destructing for protecting keys
Requiring availability and back up data services
Requiring availability and connectivity
Requiring availability, respond time and resolution time
Requiring awareness and training
Requiring business continuity plan and governance
Requiring certification and attestation of suppliers
Requiring certification and attestation of suppliers
Requiring compliance with data localisation requirements
Requiring compliance with in-house rules
Requiring compliance with standards and regulations
Requiring compliance with standards and regulations
Requiring continuous assessment
Requiring crypto tools and physical protection
Requiring cryptographic tools with standard encryption
Requiring data breach notification
Requiring data classification controls (four levels of confidentiality)
Requiring data classification controls (government data)
Requiring data classification controls (public, official and secrets)
Requiring data classification controls (three levels of confidentiality)
Requiring data classification controls and policy with appropriate security controls
Requiring data classification controls and requirements
Requiring data classification controls and standard
Requiring data encryption against interception
Requiring data encryption in process
Requiring data hiding technique
Requiring data integrity
Requiring data isolation
Requiring data leakage monitoring
Requiring data management
Requiring data protection mechanism
Requiring data retention policy and encryption
Requiring data security with AES encryption
Requiring data sharing controls
Requiring data, application, network protection
Requiring defence in depth security (people, process and technology)
Requiring digital certificate
Requiring digital signature, audit trail, non-repudiation services

Requiring disguised trustworthy entity
Requiring education records
Requiring electronic evidence and audit trails
Requiring encrypting data during processing
Requiring encrypting data during storage
Requiring encrypting data during transmission
Requiring encryption and crypto
Requiring encryption for securing communication
Requiring end-to-end communications
Requiring end-to-end supply chain contract
Requiring escalating levels of protection
Requiring explicit agreements
Requiring filtering
Requiring firewall and IDS/IPS
Requiring firewall services to control unauthorised access
Requiring frequency hopping scheme
Requiring generating keys by users
Requiring governance and compliance
Requiring governance and mitigation plan
Requiring governance and procedure
Requiring Government CA
Requiring government messenger services
Requiring grounding systems
Requiring guidance and procedure
Requiring homomorphic encryption
Requiring in-house application hosting for government agencies
Requiring in-house key management systems
Requiring in-house services
Requiring in-house technologies
Requiring in-house VPN
Requiring incident management systems
Requiring interception detector
Requiring Internet routing
Requiring isolated networks and systems
Requiring isolation and air gapping
Requiring isolation and cryptography
Requiring isolation and disconnected network
Requiring isolation from unauthorised access
Requiring IT audit and governance
Requiring IT audit, risk assessment, penetration test
Requiring key management generated by providers
Requiring key management
Requiring legal and compliance
Requiring level of protection in SLAs
Requiring liability and compliance

Requiring liability assurance for unsecured systems and networks
Requiring limited access to sensitive data and assets
Requiring local network and back up
Requiring log files and access control lists
Requiring logs access
Requiring metadata protection, digital signature and authenticity
Requiring metadata protection
Requiring methodology for securing cloud
Requiring multi factor authentication, multi people authentication
Requiring multi-factor authentication
Requiring national encryption and secure encryption
Requiring need to know access
Requiring network and computer security
Requiring network communications and secure storage
Requiring network hardening, application hardening and host hardening
Requiring network segregation
Requiring non disclosure agreements
Requiring official encrypted email communications
Requiring operation and maintenance
Requiring password management
Requiring patching software
Requiring penetration testing and code analysis
Requiring penetration testing and IT audit
Requiring penetration testing and vulnerability assessment
Requiring physical access and security
Requiring physical and logical access
Requiring physical security
Requiring physical security (CCTV), grounding systems, security controls
Requiring physical security and grounding systems
Requiring privilege access
Requiring privilege to access data stored
Requiring privileges to access sensitive data
Requiring procedure and mitigation strategies
Requiring procedure for labelling information
Requiring procedure for protecting sensitive data
Requiring public and private keys
Requiring quality of services and protection
Requiring recording logs, filtering and encryption
Requiring recovery and response efforts in handling sensitive data
Requiring regular patched software
Requiring regular security assessment
Requiring regular security audit and back up
Requiring regulations and compliance
Requiring remote secure storage
Requiring risk assessment and business continuity

Requiring risk assessment and management
Requiring risk assessment and risk analysis
Requiring Root CA
Requiring routing Internet
Requiring routing, proxy server and defence layer
Requiring sandboxing
Requiring scanning, checking vulnerabilities
Requiring secure and trusted devices
Requiring secure applications
Requiring secure channels (HTTPS)
Requiring secure cloud storage, encryption and hidden access location
Requiring secure communications with encryption
Requiring secure communications with high availability
Requiring secure communications
Requiring secure connections
Requiring secure email communications
Requiring secure encryption
Requiring secure information exchange
Requiring secure keys management
Requiring secure messaging app for government
Requiring secure software development
Requiring secure storage
Requiring secure tunnelling and end-to-end encryption
Requiring securing logs
Requiring security and usability
Requiring security assessment and procedure
Requiring security assessment and testing
Requiring security audit
Requiring security awareness
Requiring security controls, co-location and data centre, security requirements
Requiring security ethics code and conduct
Requiring security evaluation via common criteria
Requiring security governance and risk assessment
Requiring security governance and security standards
Requiring security in procurement auction
Requiring security infrastructure
Requiring security layer protection
Requiring security management process
Requiring security matrix
Requiring security module with crypto
Requiring security procurement or auction specification
Requiring security protocol (https)
Requiring security protocol (SSL/TLS)
Requiring security protocols and IPSec
Requiring security risk assessment

Requiring security standard and compliance
Requiring security standards and risk management
Requiring security standards for protecting sensitive data
Requiring security supply chain
Requiring security-related SLAs
Requiring segmentation layers
Requiring segmentation to manage Malware
Requiring segregation of duties, limited access to authorised personnel
Requiring segregation of duty
Requiring sensors (Honeynets)
Requiring service level agreements and assurance
Requiring services based on HTTPS
Requiring sharing secret code to access information
Requiring single-factor authentication
Requiring skills and expertise
Requiring source code analysis
Requiring special network paths for top secret or secret information
Requiring special network paths or communications
Requiring special routing
Requiring SSL and encryption
Requiring standard and compliance
Requiring standard for metadata protection
Requiring standard operating procedure
Requiring standard requirements by considering customised needs
Requiring steganography/data hiding
Requiring strong authentication
Requiring strong authentication when using external services
Requiring strong regulation and compliance
Requiring supply chain
Requiring support availability and risk assessment
Requiring support maintenance and segregation of duties
Requiring temper-proof and zeroisation
Requiring the use of pseudonyms to preserve anonymity and confidentiality
Requiring threat analysis
Requiring traffic monitoring
Requiring trustworthy services
Requiring uptime, bandwidth, usage, respond time
Requiring usability communications
Requiring vendor audits
Requiring virtual private network
Requiring VM
Requiring VPN for secure communication
Requiring zero knowledge access control
Requiring zero-knowledge access controls
Requiring zeroisation

Providing access cards
Providing access control
Providing authentication and authorisation
Providing CCTV
Providing compliance with laws and regulations
Providing compliance with security standards
Providing compliance with standards
Providing data breach notification
Providing data isolation
Providing downtime insurance
Providing data encryption
Providing encryption level
Providing high availability guarantees with additional security solutions
Providing isolated networks and systems
Providing identity management
Providing jitter levels
Providing key management
Providing liability assurance
Providing logs and backup services
Providing malware protection
Providing physical security
Providing penetration testing
Providing personnel security
Providing private network
Providing response time guarantees
Providing secure communications
Providing secure connections
Providing secure network using firewall, IDS and IPS
Providing Antivirus and malware protection
Providing security awareness
Providing security cages
Providing security training
Providing security training and awareness
Providing system availability (99.5%)
Providing traceability
Providing user access matrix
Providing visitor access
Providing VPN services
Providing vulnerability assessment

Presented here are the details of the memos generated during the analysis. Memos are served as a means of documenting the thoughts of the researcher throughout the analysis and thereby serve as a means of documenting reflexivity

Memos

Protecting government officials
Government officials seem to be considered as human assets. Sensitive information is usually attached to senior government officials. Of course, it is imperative to protect senior officials such as Presidents and Ministers as state assets.

Protecting knowledge and experience
Knowledge and experience seem to be considered as human assets. It is not an easy thing to be able to ensure that former state officials can maintain state secrecy or confidential information that is still attached to them. Former state officials might be barred from working for foreign companies.

Protecting intellectual property
Intellectual property seems to be protected by the laws. Any inventions and sensitive information can qualify as a secret. The government will classify more innovations as secret in the name of national security. Intellectual property is considered as a human asset to a government agency.

Protecting military and defence data
Military data is generally categorised as sensitive information, but it is also necessary to classify such information assets into a more detailed classification because not all military data is undisclosed.

Protecting personal data and privacy
Privacy and data protection seem to dominate security discussions especially regarding protecting citizen data as information assets. It is important to protect the personal data and privacy of the citizens for electronic transactions that occur within Indonesia.

Protecting health or medical records
This information is considered as sensitive data with additional protection needs. Sensitive information assets would include personal medical records.

Protecting information systems
Information systems include hardware, software, people, security and network. It is interesting to protect cyber-physical assets such things.

Protecting critical national infrastructure
The degree of sensitivity depends on the consequences if data is breached. It is important to protect critical physical assets such as data centres that store and process sensitive data.

Protecting government services
Government services are important to a government agency for delivery of public services. The key to protecting this is to safeguard physical assets that support a range of government services.

Identifying insider threats by employees
It is important to identify insider threats by employees as legitimate participants that deliberately or unwittingly cooperate with adversaries. This concept is categorised as a collaborator.

Identifying insider threats by service providers
It is interesting to know that service providers could be considered as potential insider threats when we procure services from external providers. Service providers can cooperate traitorously with an adversary.

Identifying outbound traffic
It is important to identify malicious actions that keep sending out information. The transmission of the content does deliberately or unwittingly to an attacker. An attacker will often attempt to steal sensitive data by exfiltrating it out of the government's information systems.

Identifying content exfiltration by a service provider
Data exfiltration is a malicious activity performed through various techniques, in this case by a service provider. The service provider can do content exfiltration.

Identifying interception/observation
Interception is a means of information collected directly from communications by an eavesdropper. Interception allows an adversary to intercept communications in an attempt to read sensitive government data.

Identifying discovery by foreign government
The action of the process of observing data that usually conducted by foreign intelligence services. For example, bulk metadata and access done by foreign intelligence.

Identifying a malware injection
Malware injection could steal sensitive government data. It is important to identify such a threat because it can be placed on the government's information systems through various methods.

Identifying a ransomware installation
It is important to identify the user is browsing the pages of the site that redirects them to download ransomware. Preventing ransomware installation is an active process that requires a strong combination of preventative measures and constant vigilance. Employees are not trained for security awareness is perfect for ransomware installation.

Identifying phishing attacks
Some consumers are aware of phishing, but it is important to building a tool to remind us of the importance of identifying phishing attacks.

Requiring secure communications
It is important to ensure government agencies can exchange information securely against eavesdropping, which includes using secure communications and VPNs. Secure communications are important as access management to protect sensitive government data across the broad public sector.

Requiring access control to sensitive data
Access control to sensitive data needs to be provided when processing sensitive data. It is necessary for access management to assign and enforce the access control to sensitive data. Access control restricts access from different users with different security needs and requirements.

Requiring encrypting data during processing
It is necessary to require organisations to have data management and implement data encryption in use to retain ownership and control. It provides encryption of the data at the service provider while enabling processing functionality on the encrypted data, without ever decrypting the data. Also, it enables government agencies to put sensitive data into a cloud while retaining direct ownership and control.

Requiring adequate data classification controls
Sensitive, confidential or secret information must be protected as a means of data management. The best way to accomplish this is through the use of strong data classification controls. It is important to determine whether adequate data classification exist to define sensitive government data. The responsibility for the data classification falls on the data owner.

Requiring multi-factor authentication
Multi-factor authentication is one of the most effective controls as identity management. It requires users to provide more than one form of authentication to verify identity and access systems or data.

Requiring privileges to access sensitive data
Limiting access to sensitive data is necessary. When authorised users have full privileges to access sensitive data, they can give the attacker local access if breached. It requires elevated privileges to access sensitive data throughout the government's information system.

Requiring physical security
Government data (e.g. secret) is the sensitive information requiring physical security. It is important to provide the level of security requiring physical security mechanisms to unauthorised access with malicious intent.

Requiring appropriate personnel security screening
Personnel security screening procedures are necessary as a means of malicious management. Background verification checks are carried out following the classification of the information to be accessed and the perceived risks.

Requiring compliance with standards and regulations
Compliance with standards and regulations is a fundamental requirement for governments to move to cloud-based services. Service providers must comply with government regulations to ensure data security when using external services.

Requiring certification and attestation of suppliers
The usage of certification and attestation is considered as a means of building trust between customers and providers. It expresses concern about the trustworthiness of external providers through certification.

Providing secure connections
It is important to talk about the importance of providing technical security provisions, such as secure connections for the entire government's information systems to protect sensitive data against theft and unauthorised manipulation. For example, SSL and HTTPS provide secure connections for authentication and confidentiality.

Providing encryption
It is important to provide encryption without any user action as part of technical security provisions. By doing this, it enables service providers in providing encryption by default and encryption as a service to their customers.

Providing key management
There is a need for a technical security approach for providing key management for encryption of sensitive government data. Providing key management for confidentiality is difficult due to the ad hoc nature, intermittent connectivity, and resource.

Providing malware protection
As part of technical services, malware protection is important for every network, application and website. The fundamental principle when providing malware protection is to minimise the chance of infection from known and unknown malware.

Providing CCTV
Providing CCTV services as part of physical security measures. For example, the availability of CCTV as the requirements of security services regarding physical provisions.

Providing visitor access
Providing physical controls on visitor movement and access are critical to the government's information systems to ensure resource and assets protection.

Providing security cages
Providing a suitable solution for securing assets that require a lower level of physical protection is necessary. For example security cages for servers and storage space.

Providing access cards
As part of physical security provisions, providing access cards can limit employees' access to specific areas. One of most important control is the process of providing and monitoring access cards to employees and vendors working onsite and offsite.

Providing vulnerability assessment
Vulnerability assessment focuses on uncovering as many security weaknesses as possible. It is important to know all possible security weaknesses or uncover a wide range of possible vulnerabilities.

Providing compliance with standards
Responsible for ensuring and providing compliance with standards is generally voluntary but can be mandatory when cited in legislation or regulation. Managing information security is a challenge. Traditional checklist approaches to meeting standards may well provide compliance, but do not guarantee to provide security assurance.

Providing user access matrix
It is important to define a User Access Matrix that restricts access on a contract-by-contract basis, based on an individual's assigned responsibility in the process. User access matrix is constructed based on the log, each element representing the relative number of users who accessed the resources.

Providing security training
It is important to increase the baseline of security including by providing security training.

Providing personnel security
It is important to assess the efficiency and effectiveness of the processes for providing personnel security. Service providers should have the capability of providing personnel security and facility clearance support services in the time frame required.

Appendix B

An Example of Government Tenders, Requirements and Existing SLA Provisions

1

PENGUMUMAN PELELANGAN DENGAN PASCAKUALIFIKASI

BADAN KEPEGAWAIAN NEGARA

PENGUMUMAN PELELANGAN SEDERHANA DENGAN PASCAKUALIFIKASI
Nomor : 01/UM/PPTI-C/XII/2015

Kelompok Kerja/ Panitia Pengadaan (C) Pengadaan Barang Teknologi Informasi dan Jasa lainnya di Lingkungan Badan Kepegawaian Negara TA. 2016 akan melaksanakan Pelelangan Sederhana dengan pascakualifikasi untuk paket pekerjaan pengadaan Jasa Lainnya secara elektronik sebagai berikut:

1. **Paket Pekerjaan**

Nama paket pekerjaan	:	Sewa Jaringan Komunikasi Data Leased Line dan Cloud Tahun Anggaran 2016.
Lingkup pekerjaan	:	Pengadaan Sewa Jaringan Komunikasi Data Leased Line dan Cloud, meliputi internet, intranet (WAN), dan perangkat pendukung di Lingkungan Badan Kepegawaian Negara.
Nilai total HPS	:	Rp. 4.199.709.360,-
Sumber pendanaan	:	Dibebankan pada anggaran DIPA Direktorat Pengembangan Sistem Informasi Kepegawaian Tahun Anggaran 2016 dengan kode kegiatan 088.01.06.3648.002.001.011.A.522141.

2. **Persyaratan Peserta**
   Paket pengadaan ini terbuka untuk penyedia barang/jasa yang teregistrasi pada Layanan Pengadaan Secara Elektronik (LPSE) dan memenuhi persyaratan:
   a. Memiliki izin Usaha dengan Klasifikasi Non Kecil Bidang Jasa Telekomunikasi, Internet Service Provider.
   b. Memiliki Surat Izin Operasional ISP (Jasa Akses Internet), Surat Izin Penyelenggaraan jasa interkoneksi (NAP) dan memiliki surat izin penyelenggaraan jaringan tetap tertutup.
   c. Mendapatkan pekerjaan paling kurang 1 (satu) pekerjaan sebagai penyedia barang/jasa dalam kurun waktu 4 (empat) tahun terakhir baik dikecualikan bagi yang baru berdiri kurang dari 3 (tiga) tahun.
   d. Memiliki fasilitas/peralatan/perlengkapan untuk melaksanakan pekerjaan jasa lainnya ini, yaitu: Server, router, switch (core, aggregate, NOC).
   e. TDP, PKP, Surat Keterangan Domisili Perusahaan dan NPWP yang masih berlaku serta Akte Pendirian dan perubahan terakhir.
   f. Memiliki Ijin Jaringan Tetap Tertutup sesuai dengan akses yang digunakan
   g. Memiliki Ijin ISP yang masih berlaku
   h. Memiliki ijin NAP yang masih berlaku
   i. Memiliki sertifikasi managemen mutu ISO 9001:2008
   j. Memiliki sertifikasi managemen mutu ISO 27001:2005

No	Jenis		Deskripsi	Nilai
	Link Internet Lokal			
		Koneksi ke port/gerbang Internet domestik 1 hop, menggunakan jaringan fiber optic dengan rasio bandwidth internet simetris 1:1 (minimal 200000 Kbps Lokal backbone baik ke IIX maupun ke OpenIXP), dan menggunakan tipe koneksi *upstream:downstream* adalah *BGP (dedicated, 1:1)*.	Ya	10
			Tidak	0
		Terdapat interkoneksi antara link FO di Kantor Pusat LAPAN untuk link Primer dan Sekunder sehingga bisa load balancing dan fail-over jika salah satu link mengalami gangguan (jalur fiber optic dari Primer dan sekunder wajib dicantumkan di proposal teknis)	Ya	10
			Tidak	0
		Memiliki kerjasama peering domestik dengan provider lokal. (direct peering dari AS Number Jaringan Primer dan Jaringan Sekunder harus terdaftar di IIX dan Open IXP)	Ya	5
			Tidak	0
		Jumlah link local ke NAP (kecuali NAP) > 1	Ya	5
			Tidak	0
	Interface			
		Penyediaan koneksi akses lokal dedicated dari MDF Lapan ke Penyedia Jasa menggunakan fiber optic 1 hop, terminasi/conversion di sisi user berupa dua port RJ45 / Ethernet terpisah untuk internasional dan lokal.	Ya	5
			Tidak	0
	Service Level Agreement (SLA)			
		1. Availability dari internet access, ≥ 99,5 %	≥ 99,5 %	10
			<99,5 %	0
		2. Rata rata Round trip Delay, ≤ 250 ms	= 250 ms	8
			< 250 ms	10
			>250 ms	0
		3. Packet Loss, ≤ 2 %	= 2 %	8
			< 2 %	10
			> 2%	0
		4. Respon time maksimum,	= 30 Menit	8
			< 30 menit	10
			> 30 Menit	0
		5. Rata-rata waktu recovery	= 24 Jam (Luar Jabodetabek)	8
			< 24 Jam (Luar Jabodetabek)	10
			>24 Jam (Luar Jabodetabek)	0

No	Jenis		Deskripsi	Nilai
		6. Response time maksimum di level/tier 1	= 20 menit	8
			< 20 menit	10
			>20 menit	0
		7. Resolution time maksimum link domestic	= 4 Jam	8
			< 4 Jam	10
			>4 Jam	0
		8. Resolution time maksimum link international	= 8 Jam	8
			< 8 Jam	10
			>8 Jam	0
	IP Address			
		Perpanjangan AS Number Lapan dan Blok IP Publik Lapan /24	Ya	10
			Tidak	0
		Mengadvertise 1 block IPV4 Public Class C (atas nama LAPAN), yang disediakan oleh penyedia Jaringan Primer, sehingga memungkinkan dilakukannya *fail-over* dari jaringan LAPAN, jika salah satu jaringan Primer atau jaringan Sekunder mengalami gangguan	Ya	10
			Tidak	0
Total Nilai Score Maksimum Layanan Internet				200

II. Layanan VPN

No	Jenis	Deskripsi	Nilai
2.	VPN (Virtual Private Network)		
	Memiliki Ijin Jartup dengan berbasis media yang dilayankan.	Ya	10
		Tidak	0
	Penyediaan perangkat di 23 lokasi site Lapan, yakni Router (min. Speed 800MHz, RAM 512MB, 10 LAN Port), Rak Router, dan UPS.	Ya	10
		Tidak	0
	Jaringan yang disediakan baik *lastmile* pada setiap site Lapan maupun jaringan *backbone* adalah milik Penyedia Jasa sendiri (atau mendapatkan dukungan dari Perusahaan Operator yang mendukung). Dan merupakan Jaringan yang berbeda dengan Penyedia Sekunder.	Ya	10
		Tidak	0
	Jaringan backbone milik Penyedia Jasa bersertifikat Carrier Ethernet Certification.	Ya	10
		Tidak	0

References

[1] J. T. Force and T. Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication*, vol. 800, no. 53, pp. 8–13, 2013.

[2] K.-J. Stol, P. Ralph, and B. Fitzgerald, "Grounded theory in software engineering research: a critical review and guidelines," in *Proceedings of the 38th International Conference on Software Engineering*, pp. 120–131, ACM, 2016.

[3] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing Octave Allegro: Improving the Information Security Risk Assessment Process," *Carnegie Melon University - Software Engineering Institute*, 2007.

[4] J. Nugent, "Riskmap Report 2016: Cyber Security Outlook." Available Online: `http://www.amcham.lu/uploads/tx_userevents/RM-REPORT-2016-Cyber.pdf`, 2016. Accessed 18 October 2017.

[5] W. D. Eggers, "Government's cyber challenge: Protecting Sensitive Data for the Public Good." Available Online: `https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/protecting-sensitive-data-government-cybersecurity.html`, 2016. Accessed 18 October 2017.

[6] Z. Whittaker, "Security Flaws in Pentagon Systems 'easily' Exploited by Hackers." Available Online: `http://www.zdnet.com/article/`

pentagon-system-flaws-likely-under-attack-by-foreign-hackers/, 2017. Accessed 18 October 2017.

[7] N. Lord, "Insiders vs. Outsiders: What's the Greater Cybersecurity Threat?." Available Online: https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat\-infographic, 2017. Accessed 18 October 2017.

[8] Indonesian Ministry of Communications and Informatics, "Press Release: Government Follow-up against Wiretapping." Available Online: https://kominfo.go.id/index.php/content/detail/3859/Siaran+Pers+No.+22+-PIH-KOMINFO-2-2014+tentang+Tindak+Lanjut+Kominfo+Terhadap+Masalah+Penyadapan+/0/siaran_pers, 2014. Accessed 18 October 2017.

[9] M. Brissenden, "Australia Spied on Indonesian President Susilo Bambang Yudhoyono, Leaked Edward Snowden Documents Reveal." Available Online: http://www.abc.net.au/news/2013-11-18/australia-spied-on-indonesian-president,-leaked-documents-reveal/5098860, 2014. Accessed 18 October 2017.

[10] P. Szoldra, "This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks." Available Online: http://uk.businessinsider.com/snowden-leaks-timeline-2016-9?r=US&IR=T, 2016. Accessed 18 October 2017.

[11] B. Jabour and M. Pengelly, "Australia Spied on Indonesia Talks with US Law Firm in 2013." Available: https://www.theguardian.com/world/2014/feb/16/australia-spied-indonesia-talks-us-firm, 2014. Accessed 18 October 2017.

[12] J. Risen and L. Poitras, "Spying by NSA Ally Entangled US Law Firm." Available Online: https://www.nytimes.com/2014/02/16/us/

eavesdropping-ensnared-american-law-firm.html, 2014. Accessed 18 October 2017.

[13] Y. Nugraha and A. Martin, *Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments*, pp. 57–75. Cham: Springer International Publishing: 11th IFIP WG 11.11 International Conference on Trust Management, 2017.

[14] Y. Nugraha, I. Brown, and A. S. Sastrosubroto, "An adaptive wideband delphi method to study state cyber-defence requirements," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, pp. 47–59, Jan 2016.

[15] R. Böhme, *Security Audits Revisited*, pp. 129–147. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[16] T. Klaus, *Security Metrics-Replacing Fear, Uncertainty, and Doubt*. Taylor & Francis, 2008.

[17] S. Pfleeger and R. Cunningham, "Why Measuring Security is Hard," *IEEE Security & Privacy*, vol. 8, no. 4, pp. 46–54, 2010.

[18] A. Martin, J. Davies, and S. Harris, "Towards a Framework for Security in e-Science," in *2010 IEEE Sixth International Conference on e-Science*, pp. 230–237, Dec 2010.

[19] R. Anderson, *Security Engineering*. John Wiley & Sons, 2008.

[20] S. P. Kaluvuri, M. Bezzi, and Y. Roudier, "Bringing common criteria certification to web services," in *Proceedings of IEEE Ninth World Congress on Services*, pp. 98–102, June 2013.

[21] S. P. Kaluvuri, M. Bezzi, A. Sabetta, Y. Roudier, R. Menicocci, V. Bagini, A. Riccardi, and M. Orazi, "Applying Common Criteria (CC) to Service Oriented Architectures (SOA)," in *ICCC 2012, International Common Criteria Conference, September 18-20, 2012, Paris, France*, September 2012.

[22] D. S. Herrmann, *Using the Common Criteria for IT Security Evaluation*. CRC Press, 2002.

[23] B. Duncan and M. Whittington, "Compliance with Standards, Assurance and Audit: Does This Equal Security?," in *Proceedings of the 7th International Conference on Security of Information and Networks*, SIN '14, (New York, NY, USA), pp. 77:77–77:84, ACM, 2014.

[24] M. Anisetti, C. Ardagna, E. Damiani, and F. Saonara, "A Test-based Security Certification Scheme for Web Services," *Proceedings of ACM Trans. Web*, vol. 7, pp. 5:1–5:41, May 2013.

[25] B. W. Boehm *et al.*, *Software Engineering Economics*, vol. 197. Prentice-hall Englewood Cliffs (NJ), 1981.

[26] A. Waller, I. Sandy, E. Power, E. Aivaloglou, C. Skianis, A. Muñoz, and A. Maña, "Policy based Management for Security in Cloud Computing," *Secure and Trust Computing, Data Management, and Applications*, pp. 130–137, 2011.

[27] Amazon Web Services, "AWS Cloud Compliance." Available: `https://aws.amazon.com/compliance/`, 2017.

[28] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, and U. Villano, "Security as a Service Using an SLA-Based Approach via SPECS," in *Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science*, vol. 2, pp. 1–6, Dec 2013.

[29] E. Rios, E. Iturbe, L. Orue-Echevarria, M. Rak, V. Casola, *et al.*, "Towards Self-Protective Multi-Cloud Applications: MUSA–a Holistic Framework to Support the Security-Intelligent Lifecycle Management of Multi-Cloud Applications," *SciTePress Digital Library*, 2015.

[30] S. Ready Consortium, "The SLA Ready Project Website." Available: `http://www.sla-ready.eu/`, 2015. Accessed 18 October 2017.

[31] R. Henning, "Security Service Level Agreements: Quantifiable Security for the Enterprise?," in *Workshop on New security paradigms*, pp. 54–60, ACM, 1999.

[32] B. Monahan and M. Yearworth, "Meaningful Security SLAs," *HP Labs, Bristol, Tech. Rep*, 2008.

[33] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security SLAs for Federated Cloud Services," in *Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES)*, pp. 202–209, IEEE, 2011.

[34] M. G. Jaatun, K. Bernsmed, and A. Undheim, "Security SLAs–an Idea whose Time has Come?," in *Proceedings of International Conference on Availability, Reliability, and Security*, pp. 123–130, Springer, 2012.

[35] T. Takahashi, J. Kannisto, J. Harju, S. Heikkinen, B. Silverajan, M. Helenius, and S. Matsuo, "Tailored Security: Building Nonrepudiable Security Service-Level Agreements," *IEEE Vehicular Technology Magazine*, vol. 8, pp. 54–62, Sept 2013.

[36] C. Y. Lee, K. M. Kavi, R. A. Paul, and M. Gomathisankaran, "Ontology of Secure Service Level Agreement," in *Proceedings of 16th IEEE International Symposium on High Assurance Systems Engineering*, pp. 166–172, Jan 2015.

[37] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative Reasoning About Cloud Security Using Service Level Agreements," *IEEE Transactions on Cloud Computing*, vol. 5, pp. 457–471, July 2017.

[38] A. Guesmi and P. Clemente, "Access Control and Security Properties Requirements Specification for Clouds' SecLAs," in *Proceedings of 5th IEEE International Conference on Cloud Computing Technology and Science*, vol. 1, pp. 723–729, Dec 2013.

[39] P. D. Leedy and J. E. Ormrod, *Practical Research*. 2005.

[40] B. Hancock, E. Ockleford, and K. Windridge, *An Introduction to Qualitative Research*. Nottingham - Trent Focus Froup, 1998.

[41] K. Howard, *Educating Cultural Heritage Information Professionals for Australia's Galleries, Libraries, Archives and Museums: A Grounded Delphi Study*. PhD thesis, Queensland University of Technology, 2015.

[42] T. Päivärinta, S. Pekkola, and C. Moe, "Grounding Theory from Delphi Studies," *International Conference on Infromation Systems*, 2011.

[43] O. P. Atieno, "An Analysis of the Strengths and Limitation of Qualitative and Quantitative Research Paradigms," *Problems of Education in the 21st Century*, vol. 13, pp. 13–18, 2009.

[44] R. W. Shirey, "Internet Security Glossary, Version 2," *Network Working Group - RFC 4949*, 2007.

[45] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11–33, Jan 2004.

[46] J. McCumber, "Information Systems Security: A Comprehensive Model.," in *Proceedings of the 14th National Computer Security Conference*, National Institute of Standards and Technology, 1991.

[47] R. Ross, P. Viscuso, G. Guissanie, K. Dempsey, and M. Riddle, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," *NIST Special Publication*, vol. 800, p. 171, 2015.

[48] M. Dawson, M. Eltayeb, and M. Omar, *Security Solutions for Hyperconnectivity and the Internet of Things*. Hershey - USA: IGI Global, 1st ed., 2016.

[49] V. Irish, "How to Read an NDA (Non-Disclosure Agreements)," *Engineering Management Journal*, vol. 11, pp. 111–114, June 2001.

[50] C. Ardagna, R. Asal, E. Damiani, and Q. Vu, "From Security to Assurance in the cloud: A Survey," *ACM Computing Survey*, vol. 48, pp. 2:1–2:50, July 2015.

[51] H. H. Thompson, "Why Security Testing is Hard," *IEEE Security Privacy*, vol. 1, pp. 83–86, July 2003.

[52] S. Türpe, "The Trouble with Security Requirements," in *Proceedings of 25th IEEE International Requirements Engineering Conference (RE)*, pp. 122–133, Sept 2017.

[53] R. Barnes, B. Schneier, C. Jennings, T. Hardie, B. Trammell, C. Huitema, and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement," *IETF*, 2015.

[54] J. Feigenbaum and J. Koenig, "On the Feasibility of a Technological Response to the Surveillance Morass," in *Proceedings of the 22nd International Workshop on Security Protocols, Cambridge UK*, 2014.

[55] Z. Bauman, D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. Walker, "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology*, vol. 8, no. 2, pp. 121–144, 2014.

[56] J. V. Van Hoboken, "Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era," *Me. L. Rev.*, vol. 66, p. 487, 2013.

[57] B. Toxen, "The NSA and Snowden: Securing the All-Seeing Eye," *Communications of the ACM*, vol. 57, pp. 44–51, May 2014.

[58] Amazon Web Services, "G-Cloud UK." Available Online: `https://aws.amazon.com/compliance/g-cloud-uk/`, 2016. Accessed 17 December 2017.

[59] Cabinet Office, "Procurement Policy Note-Use of Cyber Essentials Scheme Certification." Available Online: `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526200/ppn_update_cyber_essentials_0914.pdf`, Sept 2014.

[60] S. M. Hadeka, S., "DoD Amends its DFARS Safeguarding and Cyber Incident Reporting Requirements with a Second Interim Rule." Available: http://goo.gl/tvVKYk, January 2016. Accessed 18 February 2016.

[61] C. D. Heitzenrater and A. C. Simpson, "Policy, Statistics and Questions: Reflections on UK Cyber Security Disclosures," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 43–56, 2016.

[62] National Cyber Security Centre, "Implementing the Cloud Security Principles." Available: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles, 2016.

[63] P. Stanton and S. Cassidy, "DoD Further Clarifies its DFARS Cybersecurity Requirements." Available Online: https://www.insidegovernmentcontracts.com/2017/02/dod-clarifies-dfars-cybersecurity-requirements/, 2017.

[64] U. S. Government, "Federal Risk and Authorization Management Program (FedRAMP)." Available Online: https://csrc.nist.gov/csrc/media/events/ispab-february-2012-meeting/documents/feb3_fedramp_ispab.pdf, 2012. Accessed 18 October 2017.

[65] National Security Agency, "Information Assurance Technical Framework." Available Online: www.dtic.mil/dtic/tr/fulltext/u2/a606355.pdf, 2002. Accessed 17 December 2017.

[66] International Organization for Standardization, "ISO/IEC 27002: 2013: Information Technology – Security Techniques – Code of Practice for Information Security Controls," 2013.

[67] N. Lord, "What is NIST SP 800-53? Definition and Tips for NIST 800-53 Compliance." Available Online: https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53\-compliance, 2017. Accessed 6 October 2017.

[68] R. Gandhi, K. Crosby, H. Siy, and S. Mandal, "Gauging the Impact of FISMA on Software Security," *Computer*, vol. 47, pp. 103–107, Sept 2014.

[69] Centre for Internet Security, "20 CIS Critical Security Controls." Available: `https://www.cisecurity.org/controls/`, 2016. Accessed 30 September 2016.

[70] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2011.

[71] M. Mateski, C. M. Trevino, C. K. Veitch, J. Michalski, J. M. Harris, S. Maruoka, and J. Frye, "Cyber threat metrics," *Sandia National Laboratories*, 2012.

[72] B. Arkin, S. Stender, and G. McGraw, "Software Penetration Testing," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 84–87, 2005.

[73] J. D. Gilsinn and R. Schierholz, "Security Assurance Levels: a Vector Approach to Describing Security Requirements," in *Proceedings of the US DHS industrial control systems joint working group (ICSJWG) 2010 Fall Conference, Seattle, USA*, 2010.

[74] P. FIPS-140-2, "140-2: Security Requirements for Cryptographic Modules," *Information Technology Laboratory, National Institute of Standards and Technology*, 2001.

[75] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "NIST SP 800-63-3. Electronic Authentication Guideline," *National Institute of Standards & Technology*, 2013.

[76] J. Lyle, *Trustworthy Services through Attestation*. PhD thesis, University of Oxford, 2011.

[77] K. Inçki, I. Ari, and H. Sözer, "A Survey of Software Testing in the Cloud," in *Proceedings of Sixth IEEE International Conference on Software Security and Reliability Companion*, pp. 18–23, June 2012.

[78] S. Lindskog, *Modeling and Tuning Security from a Quality of Service Perspective*. Chalmers University of Technology, 2005.

[79] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST Special Publication*, vol. 800, no. 2007, p. 94, 2007.

[80] J. Spring, "Monitoring Cloud Computing by Layer, Part 1," *IEEE Security Privacy*, vol. 9, pp. 66–68, March 2011.

[81] J. Spring, "Monitoring Cloud Computing by Layer, Part 2," *IEEE Security Privacy*, vol. 9, pp. 52–55, May 2011.

[82] S. Pearson, "Toward Accountability in the Cloud," *IEEE Internet Computing*, vol. 15, pp. 64–69, July 2011.

[83] F. Doelitzscher, "Security Audit Compliance for Cloud Computing," 2014.

[84] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, vol. 53, pp. 50–58, Apr. 2010.

[85] R. A. K. Duncan and M. Whittington, "Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail," *Cloud Computing 2016*, 2016.

[86] Z. Chen and J. Yoon, "IT Auditing to Assure a Secure Cloud Computing," in *Proceedings of 6th World Congress on Services*, pp. 253–259, July 2010.

[87] E. Damiani and A. Manã, "Toward WS-Certificate," in *Proceedings of the 2009 ACM Workshop on Secure Web Services*, SWS '09, pp. 1–2, ACM, 2009.

[88] P. Unger, "Accreditation or Registration?." Available Online: `https://www.nist.gov/sites/default/files/documents/nvlap/Accreditation_vs_Registration.pdf`. Accessed 20 October 2017.

[89] U. K. Cabinet Office, "Government Ssecurity Classifications." Available Online: `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf`, 2014. Accessed 17 December 2017.

[90] D. C. Verma, "Service Level Agreements on IP Networks," *Proceedings of the IEEE*, vol. 92, pp. 1382–1388, Aug 2004.

[91] F. J. de Vaulx, E. D. Simmon, and R. B. Bohn, "Cloud Computing Service Metrics Description," *NIST Special Publication 500-307*, 2018.

[92] B. Mitchell and P. Mckee, "SLAs A Key Commercial Tool," *Innovation and the Knowledge Economy: Issues, Applications, Case Studies*, no. 4, pp. 2–2.

[93] P. Bianco, G. A. Lewis, and P. Merson, "Service level agreements in service-oriented architecture environments," tech. rep., DTIC Document, 2008.

[94] N. Karten, "With Service Level Agreements, Less is More," vol. 21, no. 4, pp. 43–44.

[95] B. Darrow, "Why the U.S. government finally loves cloud computing." Available Online: `http://fortune.com/2016/09/02/us-government-embraces-cloud/`, 2016.

[96] H. G. Hamilton, "An Examination of Service Level Agreement Attributes that Influence Cloud Computing Adoption," *PhD Thesis*, 2015.

[97] International Telecommunication Union, "ITU-T Rec. X.805 on Security Architecture for Systems Providing End-to-End Communications." Available: `https://www.itu.int/rec/t-rec-x.805-200310-i/en`, October, 2003. Accessed 18 February 2016.

[98] C. K. Chan, U. Chandrashekhar, S. H. Richman, and S. R. Vasireddy, "The Role of SLAs in Reducing Vulnerabilities and Recovering from Disasters," *Bell Labs Technical Journal*, vol. 9, no. 2, pp. 189–203, 2004.

[99] E. Gelbstein, "Data integrity—Information Security's Poor Relation," *ISACA Journal*, vol. 6, p. 20, 2011.

[100] A. D. Benedictis, V. Casola, M. Rak, and U. Villano, "Cloud Security: From Per-Provider to Per-Service Security SLAs," in *Proceedings of International Conference*

on Intelligent Networking and Collaborative Systems (INCoS), pp. 469–474, Sept 2016.

[101] V. Casola, A. Castiglione, K. K. R. Choo, and C. Esposito, "Healthcare-Related Data in the Cloud: Challenges and Opportunities," *IEEE Cloud Computing*, vol. 3, pp. 10–14, Nov 2016.

[102] B. Crespo, E. Prieto, E. Rios, M. Rak, R. C. S. P. Deussen, P. Samarati, S. K. Braun, and T. Lorunser, "Research and Innovation Challenges in Data Protection, Security and Privacy in the Cloud," January, 2016.

[103] G. Greenwald and E. MacAskill, "NSA PRISM Program Taps in to User Data of Apple, Google and Others." *The Guardian: Guardian News and Media*. Available: `https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data`, June 2013. Accessed 17 December 2017.

[104] B. Glaser, A. Strauss, and E. Strutzel, "The Discovery of Grounded Theory; Strategies for Qualitative Research.," *Nursing Research*, vol. 17, no. 4, p. 364, 1968.

[105] K. J. Stol, P. Ralph, and B. Fitzgerald, "Grounded Theory in Software Engineering Research: A Critical Review and Guidelines," in *2016 IEEE/ACM 38th International Conference on Software Engineering (ICSE)*, pp. 120–131, May 2016.

[106] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the Computer Security Practices and Needs of Journalists," in *Proceedings of 24th USENIX Security Symposium (USENIX Security 15)*, pp. 399–414, 2015.

[107] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are You Ready to Lock?," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 750–761, ACM, 2014.

[108] K. Charmaz, *Constructing Grounded Theory*. Sage, 2014.

[109] D. Dor and Y. Elovici, "A Model of the Information Security Investment Decision-Making Process," *Computers & Security*, vol. 63, pp. 1–13, 2016.

[110] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty, "Understanding Insider Threat: A Framework for Characterising Attacks," in *Proceedings of IEEE Security and Privacy Workshops*, pp. 214–228, 2014.

[111] M. Lerch and P. Spieth, "Innovation Project Portfolio Management: A Qualitative Analysis," *IEEE Transactions on Engineering Management*, vol. 60, pp. 18–29, Feb 2013.

[112] J. M. Morse, "A Review Committee's Guide for Evaluating Qualitative Proposals," *Qualitative Health Research*, vol. 13, no. 6, pp. 833–851, 2003.

[113] N. Bricki and J. Green, *A Guide to Using Qualitative Research Methodology*. 2007.

[114] N. C. Dalkey, B. B. Brown, and S. Cochran, *The Delphi Method: An Experimental Study of Group Opinion*, vol. 3. RAND Corporation Santa Monica, CA, 1969.

[115] J. Landeta, "Current Validity of the Delphi Method in Social Sciences," *Technological Forecasting and Social Change*, vol. 73, no. 5, pp. 467–482, 2006.

[116] C. Okoli and S. D. Pawlowski, "The Delphi Method as A Research Tool: An Example, Design Considerations and Applications," *Information and Management*, vol. 42, no. 1, pp. 15–29, 2004.

[117] T. Gordon and A. Pease, "RT Delphi: An Efficient,"Round-Less" Almost Real Time Delphi Method," *Technological Forecasting and Social Change*, vol. 73, no. 4, pp. 321–333, 2006.

[118] M. Turoff, "The Design of A Policy Delphi," *Technological Forecasting and Social Change*, vol. 2, no. 2, pp. 149–171, 1970.

[119] F. N. Kerlinger and E. J. Pedhazur, "Multiple Regression in Behavioral Research," *Holt, Rinehart and Winston New York*, 1973.

[120] G. W. Dickson, R. L. Leitheiser, J. C. Wetherbe, and M. Nechis, "Key Information Systems Issues for the 1980's," *MIS quarterly*, pp. 135–159, 1984.

[121] K. R. Nelms and A. L. Porter, "EFTE: An Interactive Delphi Method," *Technological Forecasting and Social Change*, vol. 28, no. 1, pp. 43–61, 1985.

[122] M. G. Stochel, "Reliability and Accuracy of the Estimation Process-Wideband Delphi vs. Wisdom of Crowds," in *Proceedings of Computer Software and Applications Conference (COMPSAC), 2011 IEEE 35th Annual*, pp. 350–359, IEEE, 2011.

[123] E. Ziglio, "The delphi Method and its Contribution to Decision-Making," *Gazing into the oracle: The Delphi method and its application to social policy and public health*, pp. 3–33, 1996.

[124] A. Stellman and J. Greene, *Applied Software Project Management*. " O'Reilly Media, Inc.", 2005.

[125] C. Hsu and B. Sandford, "Delphi Technique," in *In Neil J. Salkind (Ed.), Encyclopedia of Research Design*, pp. 344–247, SAGE Publications, 2010.

[126] J. W. Murry and J. O. Hammons, "Delphi: A Versatile Methodology for Conducting Qualitative Research," *The Review of Higher Education*, vol. 18, no. 4, p. 423, 1995.

[127] G. Rowe, G. Wright, and F. Bolger, "Delphi: A Re-Evaluation of Research and Theory," *Technological Forecasting and Social Change*, vol. 39, no. 3, pp. 235–251, 1991.

[128] R. Schmidt, K. Lyytinen, M. Keil, and P. Cule, "Identifying Software Project Risks: An International Delphi Study," *Journal of management information systems*, vol. 17, no. 4, pp. 5–36, 2001.

[129] D. Forsyth, "Delphi Technique," in *In J.Levine, & M.Hogg (Eds.), Encyclopedia of Group Processes & Intergroup Relations*, pp. 196–198, SAGE Publications, 2010.

[130] A. L. Delbecq, A. H. Van de Ven, and D. H. Gustafson, *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Scott, Foresman Glenview, IL, 1975.

[131] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? an experiment with data saturation and variability," *Field methods*, vol. 18, no. 1, pp. 59–82, 2006.

[132] C.-C. Hsu and B. A. Sandford, "The Delphi Technique: Making Sense of Consensus," *Practical Assessment, Research & Evaluation*, vol. 12, no. 10, pp. 1–8, 2007.

[133] G. J. Skulmoski, F. T. Hartman, and J. Krahn, "The delphi Method for Graduate Research," *Journal of Information Technology Education*, vol. 6, p. 1, 2007.

[134] P. Gill, K. Stewart, E. Treasure, and B. Chadwick, "Methods of data collection in qualitative research: interviews and focus groups," *British dental journal*, vol. 204, no. 6, pp. 291–295, 2008.

[135] M. C. Harrell and M. A. Bradley, "Data Collection Methods," *RAND Corporation*, 2009.

[136] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction publishers, 2009.

[137] M. J. Muller and S. Kogan, "Grounded Theory Method in HCI and CSCW," *Cambridge: IBM Center for Social Software*, pp. 1–46, 2010.

[138] I. Fléchais, *Designing Secure and Usable Systems*. PhD thesis, University College London, 2005.

[139] S. E. McGregor, F. Roesner, and K. Caine, "Individual versus Organizational Computer Security and Privacy Concerns in Journalism," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 4, pp. 418–435, 2016.

[140] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[141] M. Birks and J. Mills, *Grounded Theory: A Practical Guide*. Sage, 2015.

[142] B. G. Glaser and A. Strauss, "The Discovery of Ground Theory," *Aldine Transaction*, 1967.

[143] M. D. LeCompte and J. P. Goetz, "Problems of Reliability and Validity in Ethnographic Research," *Review of Educational Research*, vol. 52, no. 1, pp. 31–60, 1982.

[144] H. Brink, "Validity and Reliability in Qualitative Research," *Curationis*, vol. 16, no. 2, pp. 35–38, 1993.

[145] A. Strauss and J. Corbin, *Basics of qualitative research techniques*. Sage publications, 1998.

[146] W. B. Stiles, "Evaluating Qualitative Research," *Evidence-Based Mental Health*, vol. 2, no. 4, pp. 99–101, 1999.

[147] R. Rodrigo, A. Peter, H. Peter, and H. Karen, "Literature Review and Constructivist Grounded Theory Methodology," *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, vol. 16, no. 3, 2015.

[148] S. M. Kolb, "Grounded Theory and the Constant Comparative Method: Valid Research Strategies for Educators," *Journal of Emerging Trends in Educational Research and Policy Studies*, vol. 3, no. 1, p. 83, 2012.

[149] S. C. Brown, R. A. Stevens Jr, P. F. Troiano, and M. K. Schneider, "Exploring Complex Phenomena: Grounded Theory in Student Affairs Research.," *Journal of College Student Development*, vol. 43, no. 2, pp. 173–83, 2002.

[150] J. F. Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders," in *Proceedings of the Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, 2014.

[151] E. MacAskill, J. Borger, N. Hopkins, N. Davies, and J. Ball, "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." *The Guardian: Guardian News and Media*. Available: `http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa`, June 2013. Accessed 17 December 2017.

[152] J. Ball, "NSA's PRISM Surveillance Program: How It Works and What It Can Do." *The Guardian: Guardian News and Media*. Available online at: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google, June 2013. Accessed 17 December 2017.

[153] J. Ball, "NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts." *The Guardian: Guardian News and Media*. Available Online: https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls, June 2013. Accessed 17 December 2017.

[154] G. Greenwald, "NSA Tool Collects 'Nearly Everything A User Does on the Internet." *The Guardian: Guardian News and Media*. Available Online at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, June 2013. Accessed 17 December 2017.

[155] Australian Associated Press, "Australia Accused of Using Embassies to Spy on Neighbours." *The Guardian: Guardian News and Media*. Available Online: https://www.theguardian.com/world/2013/oct/31/australia-accused-embassies-spy-neighbours, October 2013. Accessed 17 December 2017.

[156] I. Brown, "The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance," *International Journal of Law and Information Technology*, vol. 23, no. 1, pp. 23–40, 2015.

[157] M. Gidda, "Edward Snowden and the NSA Files–Timeline." Available Online: https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, 2013. Accessed 17 December 2017.

[158] Council on CyberSecurity, "Critical Security Controls for Effective Cyber Defense." Available: http://www.counciloncybersecurity.org/critical-controls/, 2009. Accessed 17 December 2017.

[159] S. Hoermann, M. Aust, M. Schermann, and H. Krcmar, "Comparing Risks in Individual Software Development and Standard Software Implementation Projects: A Delphi Study," in *Proceedings of 45th Hawaii International Conference on System Science (HICSS)*, pp. 4884–4893, IEEE, 2012.

[160] International Organization for Standardization, "ISO/IEC 27001:2013, information Technology – Security Techniques – Information Security Management Systems – Requirements." Available Online: http://www.iso.org/iso/home/store/catalogue$_{i}cs/catalogue_{d}etail_{i}cs.htm?csnumber = 54534, 2013$.

[161] E. Amoroso, *Cyber Attacks: Protecting National Infrastructure*. Elsevier, 2012.

[162] Y. Nugraha and A. Martin, "Investigating SLA Confidentiality Requirements: A Holistic Perspective from the Government Agencies," *Proceedings of 11th International Conference on Emerging Security Information, Systems and Technologies*, 2017.

[163] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, pp. 269–284, June 2016.

[164] Amazon Web Services, "AWS GovCloud (US)." Available Online: https://aws.amazon.com/govcloud-us/, 2017. Accessed 17 December 2017.

[165] Government Digital Service, "Government Cloud First Policy." Available Online: https://www.gov.uk/guidance/government-cloud-first-policy, note=Accessed 17 December 2017, 2017.

[166] N. R. Cook and J. H. Ware, "Design and Analysis Methods for Longitudinal Research," *Annual Review of Public Health*, vol. 4, no. 1, pp. 1–23, 1983.

[167] J. Luna, N. Suri, M. Iorga, and A. Karmel, "Leveraging the Potential of Cloud Security Service-Level-Agreements through Standards," *IEEE Cloud Computing*, vol. 2, no. 3, pp. 32–40, 2015.

[168] D. Dor and Y. Elovici, "A Model of the Information Security Investment Decision-Making Process," *Computers & Security*, vol. 63, pp. 1–13, 2016.

[169] W. Burr, D. Dodson, and W. William, *Electronic Authentication Guideline*. US Department of Commerce, Technology Administration, NIST, 2013.

[170] T. Caddy, "FIPS 140-2," in *Encyclopedia of Cryptography and Security*, pp. 468–471, Springer, 2011.

[171] O. Diez and A. Silva, "GovCloud: Using Cloud Computing in Public Organizations," *IEEE Technology and Society Magazine*, vol. 32, pp. 66–72, Spring 2013.

[172] Amazon Web Services, "Using AWS in the context of NCSC UK's Cloud Security Principles." Available Online: `https://d0.awsstatic.com/whitepapers/compliance/AWS_NCSC_UK_Cloud_Security_Principles.pdf`, 2016. Accessed 18 October 2017.

[173] L. Taylor, "FedRAMP: History and Future Direction," *IEEE Cloud Computing*, vol. 1, pp. 10–14, Sep. 2014.

[174] C. D. Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. Campbell, and M. N. Bashir, "IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 1090–1099, May 2017.

[175] Y. Nugraha, Kautsarina, and A. S. Sastrosubroto, "Towards Data Sovereignty in Cyberspace," in *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, pp. 465–471, May 2015.

[176] F. Simorjay, "Data Classification for Cloud Readiness." Available Online: https://download.microsoft.com/download/0/A/3/0A3BE969-85C5-4DD2-83B6-366AA71D1FE3/Data-Classification-for-Cloud-Readiness.pdf, 2014. Accessed 18 October 2017.

[177] A. W. S. Services, "Introduction to AWS Security." Available Online: https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf, 2015.

[178] C. Irvine and T. Levin, "Quality of Security Service," in *Proceedings of the 2000 workshop on New security paradigms*, pp. 91–99, ACM, 2001.

[179] C. L. Paul, "A Modified Delphi Approach to a New Card Sorting Methodology," *Journal of Usability Studies*, vol. 4, no. 1, pp. 7–30, 2008.

[180] Q. Do, B. Martini, and K.-K. R. Choo, "Exfiltrating Data from Android Devices," *Computers Security*, vol. 48, no. Supplement C, pp. 74 – 91, 2015.