JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2022, 1–19
https://doi.org/10.1093/cybsec/tyac004
Research paper

Research paper

Cybersecurity service level agreements: understanding government data confidentiality requirements

Yudhistira Nugraha [1,2,*] and Andrew Martin [3]

[1]Jakarta Smart City, Department of Communications, Informatics, and Statistics, Jl. Medan Merdeka Sel. No.8-9, Jakarta Pusat, DKI Jakarta 10110, Indonesia, [2]School of Computing, Telkom University, Jl. Telekomunikasi No. 1, Terusan Buahbatu, Kabupaten Bandung, Jawa Barat 40257, Indonesia and [3]Department of Computer Science, University of Oxford, Robert Hooke Building, Parks Road, Oxford, the United Kingdom OX1 3PP, UK

*Correspondence address. E-mail: yudhistiranugraha@telkomuniversity.ac.id; andrew.martin@cs.ox.ac.uk

Yudhistira Nugraha is a senior member of the Indonesian Government, currently assigned as Director of Jakarta Smart City, Department of Communications, Informatics and Statistics—the Provincial Government of Jakarta. He has been a civil servant since 2006. He received a D.Phil. in Cyber Security from the University of Oxford. He also holds a Data Protection Officer Professional University Certificate (ECPC-B DPO) from the European Centre of Privacy and Cybersecurity (ECPC) of Maastricht University, The Netherlands. He also undertakes research and teaching in the area of cyber security, privacy and smart city at Telkom University.

Andrew Martin is a Professor of Systems Security and Director of Centre for Doctoral Training in Cyber Security at the Department of Computer Science, University of Oxford. He received the D.Phil. Degree in computer science from the University of Oxford, focusing on formal specification and verification. He has been a Faculty Member with the University of Oxford for 20 years, leading a research group studying the security of distributed systems and applications of hardware security technologies. His recent research focuses on Trusted Computing technologies, exploring how they can be applied in large-scale distributed systems, particularly cloud computing, mobile devices and the Internet of Things.

Received 6 July 2020; revised 28 December 2021; accepted 18 March 2022

Abstract

Cybersecurity requirements, such as data security, are often used as evidence for the Government's relationship with external service providers to process, store and transmit sensitive government data. However, cybersecurity researchers have not profoundly studied the practical application of government data security requirements (e.g. data confidentiality) in service level agreements (SLAs) in the context of an outsourced scenario. The relationships with external service providers are usually established through SLAs as trust-enhancing instruments. However, there is a concern that existing SLAs mainly focus on the system availability and performance aspects but overlook cybersecurity requirements (e.g. data security) in SLAs. Such an understanding is essential to develop government SLA data confidentiality requirements into the formulation of security-related SLAs. We seek to provide insights by developing and conducting a grounded adaptive Delphi method (GADM) with 35 government participants through group discussions and individual sessions. The work on the Indonesian Government's data confidentiality requirements was used as a case study. This paper provides insights into three understandings of the increasing considerations of the Government's data confidentiality requirements in SLA definitions. The three perceptions of security-related SLAs are the target of protection, the data confidentiality risks and the government SLA data confidentiality requirements. Our findings play important implications

for a better understanding of how to incorporate data confidentiality requirements according to perceived threats for government data classification in security-SLAs. Based on these findings, we recommend that the Government and service providers improve existing security-related SLAs and future research lines.

Key words: assurance, SLA, cybersecurity, data confidentiality, GADM, Indonesia

Introduction

Government agencies increasingly rely on external service providers to help support government tasks and functions using available computing, communications and storage solutions to deliver 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-based services). The level of trust with service providers is usually established through non-disclosure agreements (NDAs), certification schemes and service level agreements (SLAs) as reasonable efforts to protect sensitive government data from unauthorized access [1]. However, both NDAs and certification schemes are not well-suited to the service scenario [2]. At the same time, SLAs can serve as instruments of customer control in the service provisioning environment [3].

The existing SLA definition only pays attention to the system availability and performance aspects without expressing cybersecurity requirements (e.g. data confidentiality and integrity) in SLA contexts [4, 5, 6]. Bernsmed *et al*. [4] point out that cloud service is generally limited to availability levels and penalties due to the absence of security aspects in SLAs. Jaatun *et al*. [5] state that security aspects have usually been neglected in SLAs. Although the concept of security-related SLAs has been studied since 1999 [4, 7, 8, 9, 5, 10, 11, 12, 13], there appears to be a gap in understanding government data security requirements (e.g. data confidentiality) in SLA definitions.

Many governments have introduced a set of cybersecurity requirements in the context of government scenarios for procuring external information systems services provided by external service providers [14, 15, 16, 17]. However, academic researchers have not studied the formulation of SLA data confidentiality requirements. This gap indicates a need to understand the government SLA data confidentiality requirements when using external services from external service providers. This paper focuses on the Government's data confidentiality requirements, where potential adversaries aim to attempt unauthorized access to any sensitive data i.e. processed, stored or transmitted. However, this paper does not include other security requirements, such as data integrity and data availability.

This paper seeks to fill the gap by understanding the Government's perspective about SLA data confidentiality requirements, targeted at participants employed by or who 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 definitions. 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 Indonesian government's context. 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 categorize the extracted statements [18, 19, 20].

This paper uncovers three increasing considerations of the Government's data confidentiality requirements when defining SLAs. These insights include 21 concepts within three main categories of the protection target: human asset, information asset and physical asset. Further, 17 concepts are identified within five main categories of risk perception: collaborator, exfiltration, observation, insertion and manipulation. Finally, 22 concepts within five key government SLA confidentiality requirements are elicited: access management, data management, identity management, malicious management and compliance management.

The remainder of this paper is structured as follows. In the next section, we provide background to the study, explaining our motivation and placing the research in context. We then describe how to investigate the perception of government SLA data confidentiality requirements, including participant selection and data collection and analysis of findings. In the following we present the results of the study, and we then discuss how the findings compare with related work and provide implications for concrete recommendations and reflection on the methodology. Finally, we present the conclusion and future work.

Background and Related Work

This section briefly reviews the GADM approach to elicit government data confidentiality requirements, using Indonesia as a case study. The study on the Government's data confidentiality requirements provides insight for the inclusion of security requirements in the SLA contexts. We then provide background and gap analysis that motivate the research undertaken in this paper.

GADM approach for eliciting requirements

The GADM is a state-of-the-art research method. It combines elements of the Delphi study and grounded theory analysis that comprise simultaneous data collection and analysis, each interrelated and iterative [21]. The adaptive Delphi method aims to identify diverse opinions on individual and group responses to the specific issues [22]. We develop insights and understandings from the Delphi study data following the grounded theory analysis.

Previous studies have been conducted to develop the grounded Delphi method (GDM) [21, 23]. Moe and Paivarinta [23] deal with the challenges of information systems procurement in the Norwegian public sector. Howard [21] develops the method to explore the skills, knowledge and education needs of information system professionals in libraries and museums in Australia. This paper develops and conducts the GADM study, which varies in some respects from the two previous GDM studies [23]. Integrating grounded theory analysis and the Delphi approach with interviews and group discussions to elicit opinions on specific issues is a similarity between such methods. One of the differences is that the GADM developed in this paper uses a *Policy Delphi* approach [24]. In this paper, the adaptive Delphi

method aims not to achieve consensus but to explore diverse ideas, opinions and views regarding a specific question and generate options for consideration [24, 25]. Further, we match individual participants' different perspectives, opinions, thoughts and experiences on the research questions with greater generalizability across various participants. The grounded theory analysis used in this study is well-suited for capturing these different views from government participants in more detailed forms.

Another difference is that the GADM approach integrates elements of the Wideband Delphi method and the traditional Delphi approach, using group discussions and individual sessions [1]. The significant variance with the two previous studies in [21, 23] is that data collection is not conducted *via* email [23] or with an online questionnaire [21]. Such online questionnaires are impractical to elicit genuine opinions or thoughts from 'elite' participants, such as government participants. Instead, this paper sought to engage with government participants via focus group discussions and semi-structured interviews.

From a methodological perspective, developing the adaptive Delphi method provides a valuable means of exploring and eliciting original participants' opinions with elite participants such as government officials. This approach offers a flexible and systematic means of collecting detailed information, while maintaining validity in the research process by minimizing bias and maximizing transparency. Such an approach can also provide insights into a broader range of similar settings. Although the research method used in this study is labour-intensive and expensive, it is a practical way of investigating the Government's confidentiality requirements by using specific adaptive Delphi features, such as anonymous individual feedback, controlled feedback and group-response face-to-face meetings [1].

In summary, the adaptive Delphi method used in this paper aims to exploit the different views, opinions, thoughts and experiences of individual government participants on specified questions, with greater generalizability across various government participants. Therefore, combining the adaptive Delphi method with a detailed grounded theory analysis provides a rigorous approach to solving complex real-world problems. The grounded theory analysis used in this study is particularly well-suited for capturing such different views and opinions from participants. In this paper, the Delphi method aims to distil participants' judgment and statements through successive iterations of group discussion and individual responses and feedback. The grounded theory analysis is used to identify ways of understanding government participants' ideas and opinions.

Related work

The application of SLAs is widespread when using external information system services. However, there appears to be a gap in incorporating data confidentiality requirements into SLAs between government agencies and service providers when using external services to process, transmit or store sensitive government data. Thus, the study aims to fill the gap by understanding the Government's perspective about SLA data confidentiality requirements.

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 [26], security properties 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…(page 84)' [27].

According to Chan *et al.* [28], such security properties (i.e. availability, confidentiality, integrity, access control, authentication, non-repudiation, communication security and privacy) can be used as security SLA attributes. Availability ensures no denial of authorized access to network and service from a security perspective. For example, the authors propose a percentage of downtime due to security incidents as feasible metrics [28]. Further, Chan *et al.* [28] argue that data confidentiality and integrity are the primary security properties that can serve as security SLA attributes. However, there is little knowledge on defining metrics or levels of assurance for data confidentiality and integrity, which can be understood and accepted by customers and service providers [29]. The rest of such security properties do 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 [9], 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 [12] support the previous argument. The authors state that both the customer and the service provider need to accept statistical attributes 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.* [4] point out that incorporating security properties into explicit agreements or SLAs is essential. The authors argue that the deficiency of security properties in SLAs makes it unsuitable for service providers to deliver trustworthy services to customers, especially when service providers and other suppliers are involved in providing such services. However, the authors identify that there are still many questions about the formulation and adoption of such security-related SLAs in service provisioning. For instance, security requirements may conflict with other quality of service requirements in SLA contexts.

Also, Jaatun *et al.* [5] 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. However, the authors emphasize that formulating security-related SLAs is inadequate if the agreed terms cannot be monitored and measured.

Furthermore, Takahashi *et al.* [13] 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 capa-

Table 1: Requirements for basic technical protection from cyber attacks [14]

No	Requirement	Description
1	Boundary firewalls and Internet gateway	Information, applications and computers within the organization's internal networks **Should** be protected against unauthorized 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 authorized 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.

bilities. Moreover, the authors argue that security controls must be defined in terms of several variables in SLA contexts according to perceived risks. However, the authors point out that such security requirements and capabilities may change dynamically depending on a threat environment.

Lee *et al*. [10] 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 is necessary for customers to decide whether to procure cloud-based services to process, store and transmit such sensitive data. However, the authors point out that existing ontology-based cloud SLAs provided by service providers are difficult to understand; thus, comparing such SLAs from different service providers can also be challenging to manage.

Luna *et al*. in [11] 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 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 and requirements. Therefore, the authors propose an approach to assess security level quantitatively and 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 [8] emphasize 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 existing cloud service providers do not adequately express SLAs' security properties. Therefore, the authors introduce an approach called *a general requirement specification language*. Customers can define their security requirements regarding access controls and security properties. In contrast, cloud service providers can express their related security capabilities.

Such literature reviews provide evidence of growing awareness and application of security-related SLAs in practice. Formulating security-related SLAs in the service scenario is essential for security assurance. Although extensive research has been carried out on security-related SLAs, there appears to be a gap that adequately covers empirical studies investigating Government's data confidentiality requirements in SLA contexts. In other words, the literature still lacks insights into the question of incorporating the Government's data confidentiality requirements into SLA definitions.

Recent contracts and SLAs are found to use security controls like NIST 800–53 and ISO/IEC 27002 [30, 31]. In this case, incorporating existing security controls into SLAs constitutes security-related SLAs. However, apart from the practical approach, the inclusion of security controls in the SLA contexts does not achieve a specified security assurance level but only provides a binary assurance (compliant or non-compliant).

Several governments have addressed cybersecurity issues within supplier agreements. For example, the UK and US Governments have taken steps to reduce cybersecurity risk, especially for government procurement of external information system services [14, 15]. However, an understanding of government SLA data confidentiality requirements is little known. Thus, this section 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 10 steps of guidance, five requirements are defined [14]. 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 organization, as shown in Table 1.

It shows that the five requirements listed in CE serve as the basis upon which specific security controls define. However, Heitzenrater and Simpson [32] found that the specified technical controls do not directly map specific threats. For example, some technical controls, such as firewall and patching, can mitigate attacks by unauthorized outsiders.

Another UK initiative also outlines 14 cloud security principles in cloud computing, as shown in Table 2 [16]. Such principles are cloud security requirements for government agencies seeking to procure cloud-based services from service providers. Each principle represents a fundamental security aspect when selecting cloud services. For example, Amazon Web Services (AWS) listed on the G-Cloud Framework can provide cloud services to government agencies [33]. For this purpose, AWS provides insight into an implementation approach based on the 14 cloud security principles to make an informed decision when selecting the cloud services for handling government data classified as official information [33].

Table 2: Cloud security principles [16]

Number	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 compromized 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 authorized 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 recognizing 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 must meet 14 security requirements described in the NIST SP 800–171 standard [15, 17], as shown in Table 3. The 14 security requirements are required to protect the confidentiality of any information under applicable laws, regulations or government policies [17].

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 [34, 17]. For example, the guideline is necessary for suppliers or service providers who want to offer external services to government agencies when the offered services rely on private cloud-based services to process, store or transmit sensitive government data [35]. 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 [36].

Public procurement policy in the UK and the USA exhibits mixed evidence of incorporating security considerations when procuring services from service providers. Although the UK Government does not specify specific data confidentiality requirements that should be met by service providers [16], 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.

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, this paper investigates the practical application of government SLA data confidentiality requirements to the case of the Indonesian Government by drawing on government employees' expertise in security areas such as information security management, digital forensics, cryptography, cyber defence, malware and penetration testing.

Indonesia is an interesting case study as an emerging economy with a gross domestic product (GDP) of around IDR 9.084 trillion [1]. 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 [37, 6]. However, limited security requirements are applied to select service providers that provide external information system services to many government agencies in Indonesia.

Moreover, under Article 12, paragraph 1 of the 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 [6]. The provision of such regulation inherently implies that service providers who offer external system services are required to provide security SLAs (security-related SLAs).

However, the current provisions of SLAs focus on the system availability and performance aspects without considering security aspects [4, 38, 5]. Such SLAs also include quality of service attributes (e.g. throughput, response times, resolution times and service availability). This paper focuses on understanding government data con-

Table 3: Confidentiality requirements for government contractors [17]

No	Requirement	Description
1	Access control	Limit information system access to authorized users, processes acting on behalf of authorized users or devices
2	Awareness and training	Ensure that organizational 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 organizational 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 organizational 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 authorizing access to information systems containing CUI.
10	Physical protection	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.
11	Risk assessment	Periodically assess the risk to operations, assets and individuals.
12	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
13	System and communications protection	Monitor, control and protect organizational 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.

fidentiality requirements in formulating a SLA. However, this study does not include other security requirements, such as data integrity and data availability. 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 unauthorized access to any sensitive data i.e. processed, stored or transmitted.

Incorporating security requirements (considering data confidentiality) is difficult, especially when expressing such attributes in SLAs [4, 5] 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, cybersecurity SLAs are becoming increasingly crucial in procuring and using external information system services (e.g. cloud-based services) that handle sensitive government data.

Methodology

The RAND Corporation developed the Delphi method in the 1950s as part of a military defence project [39, 40]. This method moderates the influence of dominant individuals and follows a rigorous sequence of decision-making steps in the context of policy formulation [39]. All features of the Delphi method, such as anonymity, iteration, controlled feedback and statistical group response, elicit and refine group estimation and consensus [39, 40]. This approach avoids direct conflict among participating participants due to the absence of face-to-face communication [41].

Of specific relevance to this study, the Wideband Delphi method involves a higher level of interaction among participants than the classic Delphi method [42]. Group discussions between rounds are allowed to illuminate and explain their statements and opinions [43]. While traditional Delphi studies avoid face-to-face meetings to elicit anonymous input, the Wideband Delphi estimation can clarify the significant issues when 'judgmental information is indispensable' [41] and seek all requirements as 'informed judgement' [44]. This iterative process terminates when none of the participants wants to revise the joint estimation [22].

With this understanding, this paper develops an adaptive Delphi method based on the traditional Delphi method and the Wideband Delphi method to best engage with government participants and minimize barriers to completing the data collection activities. The research method developed in this study is a 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. This method appears as a practical way to investigate Government's data confidentiality requirements by using Delphi features, such as anonymous individual feedback, controlled feedback and group responses with face-to-face meetings [1].

Aim

This paper investigates an understanding of government SLA data confidentiality requirements using 35 government participants based in Jakarta, Indonesia, using a GADM [6]. A significant impetus for this research emerged from Article 12 of the 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 [45]. This paper's case study is limited to the Indonesian government's context; therefore, it is not applicable in other countries.

In this paper, we focus on the Government's data confidentiality requirements. Other security requirements, such as data integrity and data availability, are not included in this study. Further, this paper does not seek to express data confidentiality requirements in a legal language. Instead, it establishes an understanding of eliciting such requirements and provides insights to describe and incorporate data confidentiality requirements in SLA contexts.

A four-phase of data collection and analysis was conducted to conclude this study's objective 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 categorize the statements from participants [18, 19, 20].

Recruitment

This study began with a research proposal submitted to the Government Ministry, which administers information assurance and cybersecurity in Indonesia. After receiving 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 selection of participants is a critical aspect of a Delphi study [46]. Fundamental to Delphi studies is the understanding that group decision has great validity than those of a single person [47]. These decisions are trustworthy only if participants are knowledgeable about the research topics [47]. Further, since participants' motivations and experiences directly affect the quality of the findings, selection criteria are necessary to ensure appropriate participants contribute to study results. Rowe *et al*. [48] suggest the following criteria: ease of availability, reputation and expertise related to the research problem. Thus, the study selected participants based on participants' technical expertise with specific issues and their involvement in the policy-making process to achieve meaningful results and keep the failure rate as low as possible [46, 1].

Regarding the number of participants, there is no consensus about the optimum number of participants required for a successful Delphi study [46]. Even so, a Delphi study requires many participants to obtain divergent opinions [49]. Okoli and Pawlowski [41] suggest 10–18 participants in a Delphi group. According to the literature, the recommended number of participants varies between 5–20 people [50], 10–15 people [51] and 15–20 people [46].

In this study, we engaged with 35 of 45 invited participants. Most group discussions and individual interviews were conducted in person, although some were conducted *via* Skype. The number of participants was considered sufficient for providing a reliable analysis because 12 participants were deemed necessary to gain a comprehensive data set. We also discovered basic meta-themes after six interviews [52].

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, this study participants had diverse work experience and technical backgrounds, such as cyber defence experts, digital forensics, malware experts, cryptography experts, pen-testers and information security management experts. Additionally, most participants hold security certifications, and 12 experts have a PhD degree in information technology-related topics. Each government participant identified as P1–P35 to maintain anonymity and confidentiality. A summary of the participants is presented in Table 4.

Procedure

Each group discussion and interview within the Delphi study took between 60 and 20 min. 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 assets;
- Are there suppliers, service providers or contractors that process, store or transmit such information assets;
- 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, used for guidance to gain more information from participants. The responses to the questions were in-depth and meaningful and allowed for new themes or patterns to emerge based on actual experience.

Data collection and analysis

Many Delphi studies conduct three rounds for data collection activities [53, 54]. In practice, the first round of a Delphi study is a brainstorming phase. The subsequent round is an enrichment phase to discuss results obtained in the previous round [1]. The third round is an integration phase to combine categories that are similar in essence. In this paper, we conducted three rounds of the Delphi study, and It took several months to complete, as shown in Fig. 1:

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 to participate 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 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 [55]. The optimum number of focus group members will vary between 6 and 11 [55]. However, a focus group can work successfully in practice, with group members from 3 to 14 participants [56]. For this study, 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 previous round results. 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 32 participants

Table 4: 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			GADM study		
Identifier	General	Procurement	Cybersecurity	Round 1	Round 3	Round 2
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

Table 4: Continued

	Technical expertise			GADM study		
Identifier	General	Procurement	Cybersecurity	Round 1	Round 3	Round 2
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

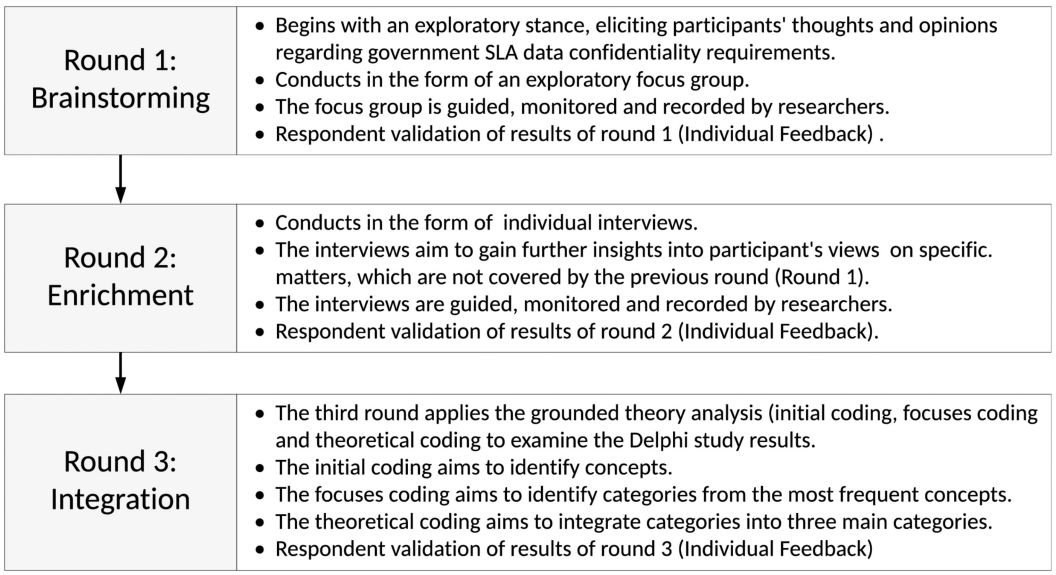

Figure 1: Phases of the GADM.

and recorded each interview in an audio format after receiving the participant's consent. Each meeting took between 20 and 120 min. 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, focused coding and theoretical coding) [18, 19, 20] to examine the Delphi study data and categorize the extracted statements. The initial coding aimed to identify concepts from which the researcher extracted useful sentences or ideas. The focus coding identified and selected categories from the most frequent or significant codes or concepts [18]. Once categories were identified, the theoretical coding aimed to integrate such categories into three increasing considerations of the Government's data confidentiality requirements in SLA definitions. The findings were sent to each participant for validation purposes, who was asked for final feedback and corrections. Therefore, the results of round 3 constitute the final results of the GADM study.

Findings

This section presents an analysis of the GADM study from our participants. In designing and analysing our study, we focused on several questions mentioned in subsection 3.3. By applying an appropriate qualitative analysis [18, 52, 20], we identify important themes and other observations present in the GADM study. Where applicable, we report the raw number of participants who discussed a particular theme to indicate its prevalence amongst participants. Our results are not quantitative; however, this paper reports the raw number of participants discussing a specific concept to indicate its prevalence. Some participants fail to mention a particular concept does not necessarily mean that it is irrelevant to such participants.

This paper introduces 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 definitions. This paper identifies emerging and essential concepts and categories present in the Delphi study data by applying a grounded theory analysis. To illustrate how this study's re-

Table 5: Target of protection. We report the number of participants who mentioned various answers for what information assets are of most value to government agencies and why are such information assets critical to government agencies. Note that some of these categories and concepts may overlap (i.e. statements and responses made by a participant may have been coded with more than one of the categories and concepts in this table)

Category	Concept	Number 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

sults were obtained, one participant commented that 'the more significant threat to government agencies mostly comes from internal sources, such as an insider threat'.

Target of protection

This study began by examining the Delphi study data from what types of government assets to protect. Several concepts were discussed by participants related to sensitive government data and assets. Therefore, this paper highlights the protection target and consolidates the concepts into human assets, information assets and physical assets, as shown in Table 5.

Human asset

Many participants agreed (15 of 35) that senior government officials were part of the protection target. Many of the participants' statements aligned with the primary category: *human assets*. The most common concept involved protecting upper-level government officials, such as the president, vice president, ministers and deputy ministers, considered protection targets.

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 paper emphasizes 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 an asset' (P8).

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

Information asset

The participants' comments 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, this study reported that each government ministry has different types of sensitive data: health or medical information (13 of 35), financial data (17 of 35), military and defence data (25 of 35), law enforcement data (10 of 35) and citizen data (13 of 25). Participants discussed that many government assets 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 from other agencies—e.g. 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, intending to build trust to the public. However, some information should not be disclosed for public consumption, such as personal data and privacy' (P2).

This study reported that the approach to protecting information consistent with its sensitivity, value and ownership should be estab-

lished to ensure protection level when processing sensitive government data.

Physical asset

Some participants reported that the Government's critical national infrastructure (5 of 35) and the Government's information systems and services (9 of 35) had to be protected from threats, resulting in exposure to liability. From a security perspective, several participants (6 of 35) focused on protecting physical, 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 protecting physical assets, as crucial as protecting 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 the protection of critical national infrastructure has huge impacts on human society, such as electricity and health facilities protecting critical national infrastructure' (P29).

This paper has identified 21 concepts within three main categories that emerged from the Delphi study data. The three categories of the protection target are (1) human asset, (2) information asset and (3) physical asset. These three types of assets, which can be found in a government organization, is fundamental to cyber security. Despite that, many governments have significant gaps in what they understand about data classification and threat environment, leading to a weakened cyber security posture. Thus, the findings have suggested that the Government and its suppliers handle sensitive government data with care and respect. However, the participants' opinion indicates an absence of government security classifications applied to government agencies that generate, process, collect, store or transmit sensitive data for conducting government activities and delivering public services. Presented below are related memos generated during the analysis.

> '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 exists to define sensitive government data. The responsibility for the data classification falls on the data owner'.

This absence of data governance and classification represents an opportunity to classify government data based on its level of sensitivity, value and criticality to the Government. Therefore, the Government should classify government data so that every entity, which works with the Government knows how best to protect sensitive data based on the data classification and threat model.

Risk perception

This subsection examines the perception of threats and risks to sensitive government data from unauthorized 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 cybersecurity 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 6.

Collaborator—allows an adversary to ex-filtrate sensitive government data or information deliberately or unwittingly from outside parties

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).

The statement above was coded as the concept of identifying an insider threat by an employee. The concept is categorized as *collaborator*. Another two participants (2 of 35) discussed insider threats from service providers; e.g. 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)

Exfiltration—It allows an adversary to obtain data or sensitive information from logs, temporary files or error messages

Many participants (14 of 35) were concerned with the illegal copying or transferring of sensitive data through various means. Participants reported that such threats allowed an adversary to perform the unauthorized 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 categorized 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 unauthorized parties' (P18).

Observation—It allows an adversary to collect credentials directly from communications in an attempt to read sensitive government data

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 encryption. Some participants reported that some

Table 6: Risk Perception. We report how many participants mentioned the perception of threats and risks to sensitive government data from unauthorized access. Participants discussed threats and risks from their concerns and real issues they have encountered

Category	Concept	Number 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

senior officials preferred meeting in person for communicating the most sensitive information.

Further, several participants (7 of 35) mentioned concern about being surveillance targets by foreign intelligence services. In contrast, 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. 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).

Insertion—It allows the adversary to inject/install/manipulate/infiltrate a message (i.e. code) onto the target device and network

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 categorized 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).

Manipulation—It allows an adversary to manipulate/modify/personate a message onto the target device, network and people

This study's participants expressed concern about phishing, spear phishing, social engineering or impersonation attacks. Participants reported that manipulating information systems was common to obtain sensitive data from targets (e.g. people). Such threats allow an adversary to pretend to be another person to collect 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 categorized 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 categorized into three groups: threat actors (*collaborator*), threat outcomes (*exfiltration, observation and manipulation*) and threat vectors (*insertion*). The threat actor can be performed by hackers, insiders, advanced persistent threats (APT) or state-sponsored attacks. However, such adversary models are not necessarily exclusive. However, risk perception categories can be applied to an area preserving the confidentiality of sensitive government data against unauthorized access.

Nugraha and Martin [6] state that understanding the perceived threats can drive security requirements. In other words, formulating security requirements play an essential role in mitigating perceived threats. However, the study reported that the Government did not know what security requirements needed to be defined and imple-

Table 7: Understanding of SLA data confidentiality requirements. We report the number of participants who mentioned various security requirements to protect sensitive government data. This table lists data confidentiality requirements discussed by participants

Category	Concept	Number 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 unauthorized 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

mented. The study also found no security requirements expressed in existing SLAs because the Government relied on the ISO 27000 series to form a strong security foundation [6].

In this paper, by understanding perceived risks and threats, we identify opportunities to provide different insights from the standard ways of eliciting and documenting security requirements against unauthorized access. Therefore, it is paramount to define government SLA data confidentiality requirements according to perceived risks to sensitive government data, especially when government agencies procure external information system services from external service providers [45, 1, 6, 57, 58].

SLA data confidentiality requirements

This subsection introduces understandings of the concepts related to the government SLA data confidentiality requirements. By identifying the specific characteristics of threats and risks against unauthorized access to sensitive government data, the concepts of SLA data confidentiality requirements were developed from the data analysis. In this paper, 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 7.

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 the transmission of sensitive government data. Interestingly, participants mentioned that protecting the integrity 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:

> '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 categorized as *access management*. As another example, participants discussed requiring access control to control or limit 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 authorized users. P15 noted the following statement:

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

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. In contrast, few participants

expressed concerns about 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 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 categorized as *data management*. As another example, most participants (22 of 35) expressed concerns about requiring adequate data classification controls to protect sensitive government data with appropriate security levels. P6 noted the following statement:

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

Identity management

Many government SLA data confidentiality requirements reported by participants were in line with authentication and authorization. The most common requirements involved requiring authentication and privileges to access sensitive data. Participants also mentioned several requirements, including requiring log files and an access control list. A total of two representative participants described data 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 cannot 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 categorized as *identity management*. In total, one participant expressed concerns about protecting 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 be stored in other countries without additional security capabilities, such as strong authentication' (P3).

Malicious management

The majority of participants (27 of 35) discussed the importance of requiring risk assessment when using external service providers' external information system services. Another major 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 security failure point. Such concepts were categorized 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).

Compliance management

Many participants (12 of 35) discussed the importance of requiring compliance with standards and regulations when procuring external service providers' external information system services. 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 the 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 impact categories: 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 localization requirements, particularly 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 organization that handles public sectors to store their data under the 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, transferred through a secure line, and should not pass through international connections. The data centre must be located in Indonesia' (P7).

Interestingly, several participants mentioned explicit requirements for building trust by using 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 22 concepts within five main categories emerging 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) compliance management. Although this paper does not seek to express data confidentiality requirements in a legal language, these findings provide insights into how the Government's data confidentiality requirements can be incorporated into SLAs. Further, these five requirements will help protect sensitive government data, whatever its size, against the most

emerging cyber threats and demonstrate the commitment to the security of data i.e. processed, collected, stored or transmitted in delivering public services.

Discussion

This section compares the findings of this study with extant literature to confirm or contradict the obtained results, elaborates on the implications of the Government's findings and makes concrete recommendations for how the findings can be used to guide the development of government data confidentiality requirements in SLA definitions. Despite the measures taken to validate and generalize findings, the ability to make generalizations 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 generalization capacity. Overall, these limitations provide opportunities for future research to build on the findings of this study.

Reflection on related works

The UK Government introduced CEs [14], which can serve as an assurance scheme for external service providers who want to conduct business with public sector government agencies. The CE requirements are identified to mitigate common successful cyber-attacks, such as malware, phishing and unpatched software in such an organization. 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, this paper's findings are designed to investigate the perception of government SLA confidentiality requirements for the Indonesian Government's context. Additionally, the study investigates the Government's data confidentiality requirements, not broadly security requirements.

The UK Government also outlines 14 cloud security principles [16], namely: data in transit protection, asset protection and resilience, the 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 the customer and secure use of the service. Such principles are used by the UK Government agencies who want to procure cloud-based services from external service providers. Again, this paper focuses on increasing an understanding of the Government's data confidentiality requirements that can be incorporated into the new definition of SLAs for the Indonesian Government. This paper's findings can be applied to various service scenarios such as cloud-based services to provide the level of security needed between government agencies and external service providers.

In the context of the US Government procurement policy, any potential and existing suppliers, service providers or contractors working with the federal agencies must meet 14 confidentiality requirements described in the NIST standard SP800-171 [15, 17]. Such requirements are 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 protecting the confidentiality of CUI when using external information system services from external service providers, the confidentiality requirements are not generally applicable to SLAs. This paper aims to increase the consideration of the Government's data confidentiality requirements in SLA definitions.

In other work, Takahashi *et al*. [13] 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 results emerged from the data, it is essential to compare the findings with extant literature to validate such findings. Moreover, Barnes *et al*. [59] introduce the confidentiality threat model into six attacker capabilities: passive observation, passive inference, active, static key exfiltration, dynamic key exfiltration and content exfiltration. Some of these categories are associated with the Delphi study categories, which are a combination of the threat actor (*collaborator*), threat outcomes (*exfiltration*, *observation* and *manipulation*) and threat vector (*insertion*). This paper identifies threats and risks to sensitive government data from unauthorized access, including threat actors, threat outcomes and threat vectors.

Furthermore, Singh *et al*. [60] 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, decentralized clouds, trust and compliance with regulations and contractual obligations. Although such security considerations are not justifiable in the Indonesian Government context, 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*. [60], the findings of this paper developed from the Delphi study data. Even so, the five main categories of government SLA confidentiality requirements are in line with the extant literature [60], namely: access management, data management, identity management, malicious management and compliance management. In essence, it is necessary to examine the extant literature with the concepts and categories that emerged from the data, as Charmaz [18] highlights the need to tailor a literature review to fit the aim of the grounded theory study.

Key take-aways

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

- The Government faces challenges related to the definition of sensitive data because each government agency has different types of sensitive government data. Such sensitive government data include health or medical, financial, tax, military and defence, law enforcement and citizen data. Thus, due to the absence of government data classifications, any entity that handles government data must adhere to a duty of confidentiality without detailed security requirements and level of protection for each data category. Thus, it is necessary to acknowledge various data handling and management constraints over the data (e.g. data protection, national security and health regulations). Further, data classification should be considered along the lines of data critical to national security, personal data, sensitive business data and publicly available data.
- The existing laws and government regulations do not give detailed security requirements, especially data confidentiality requirements for inclusion in each data classification. 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 Indonesia's context, 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.

- The Government commonly uses security controls from security standards such as ISO 27002 to ensure the confidentiality of sensitive data. On top of that, understanding the perceived threats and risks play an important role in understanding actual capabilities. It is non-trivial to classify a threat model into data confidentiality requirements to standardize the protection level necessary to manage risk from unauthorized access. Developing threat models is labour-intensive work requiring people with specific security experts who know how attacks work. Further, it is essential to enrich the expressiveness of threat model statements. It is challenging to classify threats and risks related to a particular data confidentiality requirement without an actual threat model.
- The Government finds difficulty in formulating data confidentiality requirements according to threats, especially when government agencies decide to procure external information system services to process, store or transmit sensitive data. Although the Government can obtain data confidentiality requirements from a standard enterprise security architecture or established security principles publicly available, the confidentiality requirements are not directly applicable to SLAs. Building an understanding of eliciting data confidentiality requirements is essential to describe and incorporate them in SLAs so that the government can trust the service provider. The initial formalization of government SLA data confidentiality requirements aims to provide insights of describing and placing the Government's data confidentiality requirements in SLA definition when using external information system services from service providers.
- Security-related SLAs can be formulated based on specific levels of threats and data confidentiality requirements to sensitive government data. However, it is not easy 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 incorporating appropriate protection and security requirements in SLA contexts. Thus, the Government needs to elaborate the five categories of the initial formalization of data confidentiality requirements into standard government SLA data confidentiality requirements.

Recommendations

The findings raised by this paper indicate recommendations that the Government should focus its efforts.

Government data classification levels

The Government should develop 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 data's confidentiality, integrity and availability. 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 [61] 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.

Threat capabilities

Previous works have modelled the different categories of confidentiality threat models [59, 62]. These examples of related work in the area have highlighted the need for a generalized and well-formalized threat model. It should be possible to go one stage further to capture all 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 protection and security requirements should be general to be applied to various services. Thus, it is worthwhile to investigate a set of threat models for each discrete level of protection and security requirements.

Understanding scope, risks and requirements

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 insufficient to address specific perceived and emerging threats [63]. 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 need to be defined in SLAs. By doing so, service providers can determine and negotiate appropriate data confidentiality capabilities, which demonstrate compliance with the Government's data confidentiality requirements.

Cybersecurity SLA applicability

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. Formulating the Government's data confidentiality requirements into discrete security assurance levels is the need to ensure simplicity and clarity in a security-related SLA definition. Further, it can provide sufficient practical knowledge to government organizations without requiring them to learn how to classify the Government's data confidentiality requirements according to data classification and threat environment. It also can be used to evaluate whether or not the service provider has demonstrated a set of data confidentiality requirements specified in the required level of security assurance. However, it is challenging 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 security level expressed in SLAs. These questions sketch many avenues for future work.

Reflection on the methodology

Reflection on data collection experiences

Several challenges arose during data collection activities. Firstly, although the researcher is an Indonesian civil servant, the researcher faced difficulties in convincing elite governments to participate, especially when dealing with sensitive topics and encountering uncomfortable speaking to and sharing confidential information with the researcher.

Secondly, participants sometimes felt uncomfortable when they were revealing sensitive information to the researcher. They usually did not explicitly describe such information in detail. Further, for some 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 helped obtain genuine opinions from participants.

Thirdly, the researcher faced difficulties in maintaining participant responses. During the first round of Delphi, it was difficult 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, it was good practice to perform brainstorming sessions in separate groups (comprising participants from similar expertise). Participants who were not able to attend face-to-face meetings could participate through video conferencing.

In short, such data collection activities may likely represent a challenge for other researchers who do not have good contacts with elite government participants 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.

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 [25]. As presented in this paper, during the third round of Delphi, the researcher conducted a grounded theory analysis of the Delphi study data by conducting initial coding, focused coding and theoretical coding [18] to replace a consensus or consolidated meeting, as it was expensive and difficult to hold such a meeting. The researcher borrowed its coding techniques to examine the Delphi study data to identify concepts and categories. During analysis, it took several backward steps, and such codes, concepts and categories were repeatedly corrected to conclude the report.

Overall, the essential contribution that has emerged from investigating Government's data confidentiality requirements is a methodology that addresses the specific limitations of engaging with senior officials from the Government and the private sector, all of whom have security postures to protect. Combining these two approaches allows the researcher to gain additional validity from the results as both methodologies complement each other. The adaptive Delphi method helps obtain 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.

A final criticism can be directed to the methodology used in this study, including research design, setting and participant, data collection technique and data analysis. Despite the measures taken to validate and generalize findings, the ability to make generalizations 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 concepts and categories of understanding government data confidentiality requirements, with more capacity for generalization. Overall, these limitations provide opportunities for future research to build on the findings of this study.

Conclusion and Future Work

This paper has investigated the understanding of government SLA data confidentiality requirements for the context of the Indonesian Government. This study's findings provide insights for the Government in understanding and formulating government data confidentiality requirements in a security-related SLA definition. These findings have introduced three perceptions of security-related SLAs, which are: the perception of the target of protection, the perception of the data confidentiality risks and the perception of the government SLA data confidentiality requirements. We have compared the findings of this study (concepts and categories) with related works and literature, and such results are associated with the theory and concept of data security.

Moreover, this paper's findings indicate that understanding government SLA confidentiality requirements has seen limited demand for service provisions in government contracts, especially relating to external information system services supplied by external service providers. The fact that Government relies on the requirements of ISO/IEC 27001. This research area has not been studied in depth by the academic security community because this study conducted in this paper was labour-intensive and time-consuming. This study required support from the Government for data collection activities, especially eliciting and placing Government's requirements onto service providers in the context of an outsourced situation.

The evidence from this paper concludes that classifying government data is important to define what to protect, so that perceived threats and risks can be managed through data classification. Identifying data confidentiality threats and risks can then define government SLA data confidentiality requirements. In so doing, this paper has established an understanding of eliciting such requirements and providing insights to describe and incorporate data confidentiality requirements in SLA contexts.

Furthermore, the standardization of such provisions is an essential direction for future research. Although such security requirements presented in NIST SP 800–171 are mainly concerned with protecting the confidentiality of CUI 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 paper and future work aim to increase the consideration of the Government's data confidentiality requirements in SLA definitions when using external information system services from service providers. Therefore, future work needs to elaborate such requirements into a general government SLA data confidentiality requirement through engagement with a group of participants from each government agency across Indonesian government agencies.

Our findings provide insights into how government data confidentiality requirements can be incorporated into a security-related SLA. We also find that the existing legal framework does not give de-

tailed government data confidentiality requirements for inclusion in each data classification and threat environment. This mismatch provides a significant opportunity to advance the understanding of incorporating the Government's data confidentiality requirements based on discrete security assurance levels as the basis for constructing a legal language in SLAs.

In terms of methodology, the applicability of GADM should be considered in this respect. This research approach is suitable for developing standard government data confidentiality requirements. However, such research activities may challenge some researchers who do not have good contacts with elite government experts. 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.

On top of that, we argue that GADM enhances the Delphi method by providing a practical means of exploring and eliciting original participants' views and opinions with elite government participants. This method provides a flexible and systematic means of collecting detailed information while maintaining validity in the research process by minimizing bias and maximizing transparency. At the same time, the grounded theory analysis provides a rigorous means of identifying and selecting key concepts and core categories from patterns in the Delphi data, and creates relationships between the conceptual categories identified with the prioritized research questions.

Our future research efforts are focused on enhancing the Delphi method. In particular, we aim to study whether the participants would feel unnecessarily pressured to discuss the results of GADM Round 3 and give a review and feedback in a relatively short amount of time in terms of theorizing, linking with the development of concepts and categories and thinking about methodologies. The availability of qualified participants does not directly fit with other data collection processes. Thus, we regard GADM mainly as an enhancement and extension of the grounded Delphi method, which brings rigour to theory development which can be grounded upon Delphi data collected from qualified participants who understand the issues related to the problems of understanding cybersecurity requirements in SLAs.

Acknowledgements

The authors thank Dr Will Tibben (University of Wollongong, Australia) for the thought-provoking discussions and feedback on this manuscript's draft. The authors also would like to thank the anonymous experts for their participation in this study. The views expressed in this paper are those of the authors and do not reflect the official policy or position of the Government of Indonesia. Any errors, of course, remain our responsibility.

References

1. Nugraha Y, Brown I, Sastrosubroto AS. An adaptive wideband Delphi method to study state cyber-defence requirements. *IEEE Trans EmergTop Comput* 2016;**4**:47–59.
2. Anisetti M, Ardagna CA, Damiani E. *et al.* A test-based security certification scheme for web services. *Proc ACM Trans Web* 2013;**7**:5. 1–5:41.
3. Spring J. Monitoring cloud computing by layer, part 1. *IEEE Secur Priv Mag* 2011;**9**:66–8.
4. Bernsmed K, Jaatun MG, Meland PH. *et al.* Security SLAs for federated cloud services. In: *Proceedings of the Sixth International Conference on Availability, Reliability and Security (ARES)*, p.202–209. Washington, DC: IEEE, 2011.
5. Jaatun MG, Bernsmed K, Undheim A. Security SLAs–an idea whose time has come?. In: *Proceedings of International Conference on Availability, Reliability, and Security*, p.123–30. Berlin, Heidelberg: Springer, 2012.
6. Nugraha Y, Martin A. Investigating security capabilities in service level agreements as trust-enhancing instruments. In: *Proceedings of the Eleventh IFIP WG 11 International Conference on Trust Management*. p.57–75. Cham: Springer International Publishing, 2017.
7. Butkovic MJ. *Cybersecurity SLAs: Managing Requirements at Arm's Length*. 2013. https://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_54269.pdf(18 October 2017, date last accessed).
8. Guesmi, Clemente P. Access control and security properties requirements specification for clouds' SecLAs. In: *Proceedings of Fifth IEEE International Conference on Cloud Computing Technology and Science*. **Vol. 1**, p.723–9, IEEE, Bristol: 2013.
9. Henning RR. Security service level agreements: quantifiable security for the enterprise?. In: *Proceedings of the Workshop on New security paradigms*, p.54–60. New York, NY: ACM, 1999.
10. Lee CY, Kavi KM, Paul RA. *et al.* Ontology of secure service level agreement. In: *Proceedings of the Sixteenth IEEE International Symposium on High Assurance Systems Engineering*, p.166–72, Daytona Beach Shores, FL: IEEE.2015.
11. Luna J, Taha A, Trapero R. *et al.* Quantitative reasoning about cloud security using service level agreements. *IEEE Trans Cloud Comput* 2017;**5**:457–71.
12. Monahan B, Yearworth M. Meaningful security SLAs. Technical Report, Bristol: HP Labs, 2008.
13. Takahashi T, Kannisto J, Harju J. *et al.* Tailored security: building non-repudiable security service-level agreements. *IEEE Veh Technol Mag* 2013;**8**:54–62.
14. Cabinet Office. *Procurement Policy Note-Use of Cyber Essentials Scheme Certification*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526200/ppn_update_ cyber_essentials_0914.pdf, Sept 2014. (17 December 2017, date last accessed).
15. Hadeka S, Scheimer M. *DoD Amends its DFARS Safeguarding and Cyber Incident Reporting Requirements with a Second Interim Rule*. 2016. http://goo.gl/tvVKYk(18 February 2016, date last accessed).
16. National Cyber Security Centre. *Implementing the Cloud Security Principles*. 2016. https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles. (17 December 2022, date last accessed).
17. Ross R, Viscuso P, Guissanie G. *et al.* Protecting controlled unclassified information in nonfederal information systems and organizations. *NIST Spec Publ* 2015;**800**:171.
18. Charmaz K. *Constructing Grounded Theory*. Thousand Oaks, CA: SAGE Publications, 2014.
19. Egelman S, Jain S, Portnoff RS. *et al.* Are you ready to lock?. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, p.750–61. New York, NY: ACM, 2014.
20. McGregor SE, Charters P, Holliday T. *et al.* Investigating the computer security practices and needs of journalists. In: *Proceedings of Twenty-Fourth USENIX Security Symposium (USENIX Security 15)*, p.399–414, Washington, DC: USENIX, 2015.
21. Howard K. *Educating Cultural Heritage Information Professionals for Australia's Galleries, Libraries, Archives and Museums: A Grounded Delphi Study*. Ph.D. thesis, Queensland University of Technology, 2015.
22. Stellman A, Greene J. *Applied Software Project Management*. Newton, MA: O'Reilly Media, Inc., 2005.
23. Paäivaärinta T, Pekkola S, Moe C. Grounding theory from Delphi studies. In: *Proceedings of the International Conference on Information Systems*, Shanghai: ICIS, 2011.
24. Turoff M. The design of a policy Delphi. *Technol Forecast Soc Change* 1970;**2**:149–71.
25. Hsu C-C, Sandford BA. The Delphi technique: making sense of consensus. *Pract Assess Res Evaluat* 2007;**12**:1–8.
26. International Telecommunication Union. *ITU-T Rec. X.805 on Security Architecture for Systems Providing End-to-End Communications*. 2003. https://www.itu. int/rec/t-rec-x.805-200310-i/en(18 February 2016, date last accessed).
27. Schneier B. *Secrets and Lies: Digital Security in a Networked World*. Hoboken, NJ: John Wiley & Sons, 2011.

28. Chan CK, Chandrashekhar U, Richman SH.. *et al.* The role of SLAs in reducing vulnerabilities and recovering from disasters. *Bell Labs Tech J* 2004;**9**:189–203.
29. Gelbstein Ed. Data integrity—information security's poor relation. *ISACA J* 2011;**6**:20.
30. Rak M, Suri N, Luna J. *et al.* Security as a service using an SLA-based approach via SPECS. In: *Proceedings of the Fifth IEEE International Conference on Cloud Computing Technology and Science*. **Vol. 2**, p. 1–6, Bristol: IEEE, 2013.
31. SLA Ready Consortium. *The SLA Ready Project Website*. 2015. http://www. sla-ready.eu/(18 October 2017, date last accessed).
32. Heitzenrater CD, Simpson AC. Policy, statistics and questions: reflections on UK cyber security disclosures. *J Cybersecur* 2016;**2**: 43–56.
33. Amazon Web Services. *G-Cloud UK*. 2016. https://aws.amazon. com/compliance/g-cloud-uk/(17 December 2017, date last accessed).
34. Joint Task Force and Transformation Initiative. *Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: NIST Special Publication, 2013;**800**:8–13.
35. Stanton P, Cassidy S. *DoD Further Clarifies its DFARS Cybersecurity Requirements*. 2017. https://www.insidegovernmentcontracts.com/2017/02/dod-clarifies-dfars-cybersecurity-requirements/. (17 December 2022, date last accessed).
36. US Government. *Federal Risk and Authorization Management Program (FedRAMP)*. 2012. https://csrc.nist.gov/csrc/media/events/ispab-february-2012-meeting/documents/feb3_fedramp_ispab. pdf(18 October 2017, date last accessed).
37. LPKPP. *Procurement of Government Goods and Services*. 2010. https://jdih.lkpp.go.id/regulation/peraturan-presiden/peraturan-presiden-nomor-54-tahun-2010(05 Feb 2021, date last accessed).
38. Hamilton HG. *An examination of service level agreement attributes that influence cloud computing adoption*. Ph.D. Thesis, Nova Southeastern University, 2015.
39. Dalkey NC, Brown BB, Cochran S. *The Delphi Method: An Experimental Study of Group Opinion*, **Vol. 3**. Santa Monica, CA: RAND Corporation. 1969.
40. Landeta J. Current validity of the Delphi method in social sciences. *Technol Forecast Soc Change* 2006;**73**:467–82.
41. Okoli C, Pawlowski SD. The Delphi method as a research tool: an example, design considerations and applications. *Inf Manag* 2004;**42**:15–29.
42. Stochel MG. Reliability and accuracy of the estimation process-wideband Delphi vs. wisdom of crowds. In: *Proceedings of the 2011 IEEE Thirty-Fifth Annual Computer Software and Applications Conference (COMPSAC)*, p.350–9. Washington, DC: IEEE, 2011.
43. Boehm BW. *Software Engineering Economics*, **Vol. 197**. Englewood Cliffs, NJ: Prentice-hall, 1981.
44. Ziglio E. The Delphi method and its contribution to decision-making. In: *Gazing into the Oracle: The Delphi Method and its Application to Social Policy and Public Health*, p.3–33, London: Jessica Kingsley Publishers, 1996.
45. KOMINFO. *Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Teransaksi Elektronik*. 2012. https: //jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+ pemerintah+republik+indonesia+nomor+82+tahun+2012(05 Feb 2021, date last accessed).
46. Hsu C, Sandford B. Delphi technique. In: Salkind N J. (ed.), *Encyclopedia of Research Design*, p.344–247. Thousand Oaks, CA: SAGE Publications, 2010.
47. Murry JW, Hammons JO. Delphi: a versatile methodology for conducting qualitative research. *Rev High Educ* 1995;**18**:423.
48. Rowe G, Wright G, Bolger F. Delphi: a re-evaluation of research and theory. *Technol Forecast Soc Change* 1991;**39**:235–51.
49. Schmidt R, Lyytinen K, Keil M. *et al.* Identifying software project risks: an international delphi study. *J Manag Inf Syst* **17**:5–36, 2001.
50. Forsyth D. Delphi technique. In: Levine J., Hogg M. (eds.), *Encyclopedia of Group Processes & Intergroup Relations*, Thousand Oaks, CA: SAGE Publications, 2010, 196–8.
51. Delbecq AL, Van de Ven AH, Gustafson DH. *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Glenview, IL: Scott Foresman, 1975.
52. Guest G, Bunce A, Johnson L. How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, **18**:59–82, 2006.
53. Schmidt R, Lyytinen K, Keil M. *et al.* Identifying software project risks: an international Delphi study. *J Manag Inf Syst* 2001;**17**:5–36.
54. Skulmoski GJ, Hartman FT, Krahn J. The Delphi method for graduate research. *J Inf Technol Educ Res* 2007;**6**:001.
55. Harrell MC, Bradley MA. *Data Collection Methods*. Santa Monica, CA: RAND Corporation, 2009.
56. Gill P, Stewart K, Treasure E. *et al.* Methods of data collection in qualitative research: interviews and focus groups. *Br Dent J* 2008;**204**:291–295.
57. Nugraha Y, Martin A. Investigating SLA confidentiality requirements: a holistic perspective from the government agencies. In: *Proceedings of the Eleventh International Conference on Emerging Security Information, Systems and Technologies*, Rome: International Academy, Research, and Industry Association (IARIA), 2017.
58. Nugraha Y, Martin A. Towards the classification of confidentiality capabilities in trustworthy service level agreements. In: *Proceedings of the 2017 IEEE International Conference on Cloud Engineering (IC2E)*, p. 304–10, Vancouver, BC: IEEE, 2017.
59. Barnes R, Schneier B, Jennings C. *et al. Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement*. Fremont, CA: IETF, 2015.
60. Singh J, Pasquier T, Bacon J. *et al.* Twenty security considerations for cloud-supported internet of things. *IEEE Internet of Things J* 2016;**3**:269–84.
61. UK Cabinet Office. *Government Ssecurity Classifications*. 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/ Government-Security-Classifications-April-2014.pdf(17 December 2017, date last accessed).
62. Do Q, Martini B, Choo K-KR. Exfiltrating data from android devices. *Comput Secur* 2015;**48**:74–91.
63. Boähme R. *Security Audits Revisited*, Berlin, Heidelberg: Springer, 2012, 129–47.