Towards a framework for trustworthy data security level agreement in cloud procurement

Yudhistira Nugraha[a,b], Andrew Martin[c]

[a]*School of Computing - Telkom University, Indonesia*
[b]*Jakarta Smart City, Department of Communications, Informatics, and Statistics, Indonesia*
[c]*Department of Computer Science, University of Oxford, the United Kingdom*

Abstract

After the post-Snowden upheavals, there is a growing concern about preserving the confidentiality of sensitive data across government agencies when using global cloud service providers, such as Amazon Web Services and Microsoft Azure. The use of certification schemes is becoming more critical to assure the security of services offered. This situation is problematic because many certification schemes aim to demonstrate compliance with a security standard rather than achieve a specified security level. Despite the benefits of security certification schemes like Common Criteria (CC), an assurance-based certification process does not scale well to service provision. To this end, this paper aims to investigate the concept of system assurance and trustworthiness in service provisioning, especially when government agencies procure cloud-based services. By using work on the Indonesian Government's data confidentiality requirements, this work develops principles as foundations for *a trustworthy data security level agreement (TDSLA) capability framework* as a new assurance mechanism for service provisioning based on discrete levels of security assurance incorporated into the formulation of a service level agreement (SLA). The principles which have emerged from the empirical qualitative data collection were evaluated and validated using four approaches, namely: 1) reflection against related work; 2) testimonial validity through participants' feedback; 3) use cases, and 4) application of transferability using cases from the UK Government Cloud (G-Cloud) and the US Federal Risk and Authorization Management Program (FedRAMP). The TDSLA capability framework can form the basis for constructing a legal language in contracts or SLAs.

Keywords:
Security, Assurance, Trustworthy Data Security Level Agreement (TDSLA), Service Level Agreement, Cloud Services, Government Procurement, Indonesia

1. Introduction

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

Nugraha et al.[1] show that government security needs, such as non-disclosure agreements (NDAs), trustworthy system certifications, and information security agreements, have been proposed to address security within supplier agreements. However, both NDAs and certification schemes are not well suited to the service scenario because such schemes do not fit into dynamic environments[2] and are not sufficient to address emerging threats and vulnerabilities in a dynamic threat environment[3, 4]. Furthermore, the information security agreement is solely for mutual trust and understanding of the restricted use of confidential material, knowledge, or information between parties. In contrast, the research and development into security clauses in contracts and SLAs are still ongoing.

Debate continues about a tailored and appropriate assurance approach in service provisioning. The reason is that the objective of certification schemes is to help ensure compliance with a security standard rather than achieve a meaningful level of security [5, 6]. Therefore, this paper aims to develop the concept of system assurance and trustworthiness when using external information system services, such as cloud-based services. The application of assurance-based SLAs is essential when using such external services. However, the provision of SLAs only pays attention to the performance and system availability aspects without considering data confidentiality when processing, transmitting, or storing sensitive government data [7, 8]. Although extensive research has been carried out on the formulation of security-related SLAs [7, 9, 8, 10, 11, 12, 13, 14, 15], there appears to be insufficient coverage of incorporating the Government's data confidentiality requirements into SLAs when using external information system services.

Due to the lack of assurance on the security of information system services in previous studies, the work on the Indonesian Government's data confidentiality requirements provides guidance in developing foundations from the empirical qualitative data derived from the two Delphi studies, each conducted with different participant groups. The first Grounded Delphi study was conducted by asking 35 government participants via group

discussions and individual sessions [16]. The second Grounded Delphi study[4] was performed by inviting 15 participants from the five selected service providers that provide external information system services to government agencies.

Therefore, this paper presents principles as foundations for a TDSLA capability framework that can provide a significant opportunity to advance the understanding of incorporating the Government's data confidentiality requirements into SLAs. It is necessary to clarify what characterises the different levels for each data classification and threat environment. Government requirements should be transparent in a legal language. Hence, the TDSLA framework can form the basis for constructing a legal language in SLAs.

The main contributions of this paper are as follows:

- Developing principles as foundations for a TDSLA capability framework;
- Describing discrete levels of security assurance that can be incorporated into SLAs; and
- Validating the framework with real-world cases and through participants' feedback.

The remainder of this paper is structured as follows. Section 2 discusses the background and related work. The next section presents the methodology used to define the principles and framework. Section 4 presents principles as foundations for a TDSLA capability framework. Section 5 validates the principles and framework using participants' feedback and real-world cases. Finally, Section 6 presents a discussion and conclusion.

2. Background and related work

This section provides a brief review of a Delphi approach to develop principles as foundations for a TDSLA capability framework between government agencies and service providers, using Indonesia as a case study. The work on the Government's data confidentiality requirements serves as the context of empirical data collection to support the investigation, development, and evaluation of foundations for a TDSLA capability framework. We then provide background and gap analysis that motivate the research undertaken in this paper.

2.1. GADM Approach in Developing Framework

The methodology adapted for this study combines elements of the Delphi method and grounded theory. The Delphi method and grounded theory consist of simultaneous data collection and analysis, with each process being interrelated and iterative [17]. The Delphi method aims to identify diverse opinions on specific questions as part of individual and group responses [18]. In contrast, the grounded theory aims to develop a theory or framework from the Delphi study data.

The grounded adaptive Delphi method (GADM) is a new research method. However, several attempts have been made to develop such a method. For instance, Moe and Paivarinta deal with the challenges of information systems procurement in the Norwegian public sector [19]. Similarly, Howard [17] explores the skills, knowledge, and education needs of information professionals in galleries, libraries, archives, and museums (GLAM) in Australia.

This paper employs the recently developed GADM, which varies in some respects from the two previous GDMs [17] and [19]. A significant similarity between such methods is integrating grounded theory analysis and the Delphi method with group discussions and interviews to elicit opinions on specific problems. However, one of the differences is that the GADM approach used a Policy Delphi approach [20]. The Delphi method's objective is not to achieve consensus but to explore diverse ideas, opinions, and views regarding a specific question and generate options for consideration [20]. The adaptive Delphi method aims to suit the different views, opinions, thoughts, and experiences of individual participants on specific matters, with greater generalisability across various participants. The grounded theory analysis is particularly well-suited for capturing these different views from participants in more detailed forms.

Another distinction is that the GADM approach combines elements of the Wideband Delphi method and the traditional Delphi approach, using group discussions and individual sessions [1]. The most significant difference with the previous studies in [17][19] is that data collection is not conducted via email [19] or with an online questionnaire [17]. Such online questionnaires are impractical to elicit genuine opinions or thoughts from 'elite' participants, such as government participants. Instead, this study sought to engage with participants via focus groups and semi-structured interviews.

2.2. Related Work

Preserving the confidentiality of sensitive government data has grown in importance after the secret documents made public by Edward Snowden, particularly about the NSA's PRISM surveillance program [21]. Many governments doubt the policy of procuring external information system services like cloud-based services, primarily supplied by US companies.

Many certification schemes have become essential for government procurement and tender processes to help identify levels of security for information systems [3] because measuring levels of security products, systems, and services is a hard problem [22, 23]. For example, Common Criteria (CC) is often used as the basis for a government-driven certification scheme and security evaluation for information technology products and systems [24]. Such a certification scheme is designed for public procurement to certify levels of security for products that range from hardware to software and firmware [3, 5].

However, the CC certification is an expensive process and known to be slow-moving as evaluation takes up to 12 months [5, 25]. Additionally, the CC certification only focuses on the technical elements of the products and systems. In contrast, other security elements, such as administrative and legal aspects, are overlooked [5]. Moreover, the certification of commercial products is questionable because the contexts of application are different

from those used to evaluate the products [5]. These flaws can directly result from a lack of interest from service providers to consider the CC certification scheme for services seriously. Although several studies have examined the application of CC to service scenarios [26, 25], very few services make use of the CC certification scheme [26, 27]. Consequently, it can be argued that such a certification is inappropriate in the context of service provision.

Another certification for public procurement is based on the industry-standard ISO/IEC 27001 [3, 5]. Such certification is a requirement for public procurement-related services and information technology systems for Indonesian government agencies [4]. However, the certification scheme is intended for certifying information security management systems (ISMS) for a specific scope but not suited to addressing emerging threats and vulnerabilities. Instead, it is more likely to ensure compliance with a particular security standard than achieve a significant level of security for products, systems, and services [6, 5, 3]. Overall, this explains that certification schemes to both products and services face a problem with a dynamic threat environment. It can be concluded that the certification schemes are not well-suited to the service scenario because certifications do not fit into a dynamic threat environment [2].

Several attempts have been made to express security properties in SLA contexts [7, 9, 8, 10, 11, 12, 13, 14, 15]. However, the importance of SLA-based discrete levels of assurance is still not adequately considered when service providers are handling sensitive government data and assets. Moreover, the literature still lacks insights into incorporating the Government's data confidentiality requirements into SLAs according to the data classification and threat model. On top of that, the literature review presented thus far provides evidence that there are growing awareness and application of security-related SLAs in practice. The formulation of security-related SLAs in the service scenario is an essential foundation of security assurance.

Although extensive research has been carried out on security-related SLAs, there appears to be a gap that adequately covers empirical studies on investigating government's data confidentiality requirements in SLA contexts. Recent contracts and SLAs are found to use security controls like NIST 800-53 and ISO/IEC 27002 [13, 15]. In other words, 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 level of security assurance but instead only provides a binary assurance (compliant or non-compliant).

Therefore a research opportunity exists to advance the state-of-the-art by elaborating and formulating such security controls to discriminating levels of security assurance which is of utmost significance for incorporating the Indonesian Governments' data confidentiality requirements into SLAs between government agencies and service providers. Due to the lack of understanding of the concept of system assurance and trustworthiness, especially when government agencies procure and use external information system services from service providers, this paper seeks to fill this gap and present principles as foundations for a TDSLA capability framework. The original inspiration for building a TDSLA capability framework is the CC certification process. CC aims to certify levels of security for products. In contrast, the TDSLA capability framework aims to certify levels of security for services.

3. Methodology

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

Due to the lack of previous studies on the concept of assurance in service provisioning, a qualitative analysis based on the grounded theory approach was conducted to develop principles and framework from the data derived from two empirical studies in [4][16]. Each empirical study was conducted in different settings and participant groups. The grounded theory approach is a well-established research methodology by which a proposed framework can be developed through a process of data collection activities, coding, and categorisation. This is followed by several comparative and theoretical analyses of findings [28, 29, 30, 31, 32, 33].

Using grounded theory has the advantage of being a systematic but flexible approach to analysing qualitative data. Additionally, this method can analyse complex social phenomena and experiences [30, 34]. Consequently, the grounded theory is a practical approach to developing principles and a framework from the data. However, using the grounded theory approach has limitations. The researcher might be biased, a misinterpretation of coding procedures, and single case study with limited participants. Some steps have been taken to minimise the influence of these limitations. Despite the limitations of the research method, grounded theory is a suitable technique to present principles as foundations for a TDSLA capability framework because of an iterative development process.

3.1. Data Collection

Two empirical studies were conducted in [16, 4] with a total of 50 participants to explore opinions on how to incorporate the Government's data confidentiality requirements into SLA contexts.

Government Agencies

A set of data collection activities were conducted with 35 government participants [P1-GOV, P2-GOV,..., P30-GOV] via focus group and individual sessions within the scope of the Delphi data collection rounds [16]. The study selected participants

based on participants' technical expertise and their involvement in the policy-making process to achieve meaningful results and keep the failure rate as low as possible [1]. Overall, this study engaged 35 of 45 invited participants. Most group discussions and individual interviews were conducted in-person, although some were conducted via Skype.

In this study, participants were civil servants and government consultants working with the Indonesian government. This focus aimed to explore the problem of preserving the confidentiality of sensitive data across government agencies. Further, the participants of this study had diverse work experience and technical backgrounds, such as cyber defence experts, malware experts, cryptography experts, pen-testers, and information security management experts. Additionally, most participants hold security certifications, and 12 participants hold a Ph.D. degree in information technology-related topics. Each participant identified as P1 to P35 to maintain anonymity and confidentiality.

The Delphi study took several months to complete. It consisted of three rounds of the Delphi study, as shown in Figure 1:

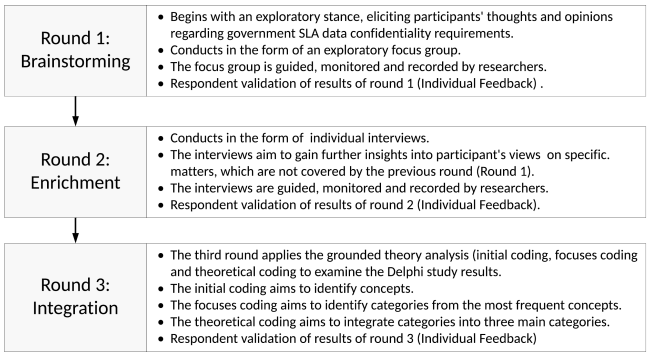

Figure 1: GADM with 25 Government Participants

Service Providers

A longitudinal study was carried out using a dataset on government procurement of 59 e-procurement services across 80 government agencies to identify major service providers that provided Internet services, cloud-based services, and data centre services to Indonesian government agencies. The longitudinal study was designed to increase the precision of selecting service providers and identify the winners of government auctions each financial year. Based on the longitudinal study results, the selected service providers were identified and selected according to the number of bids won and the value of the procurement project handled by service providers. This process is a rationale for selecting the selected service providers. Lastly, the five selected service providers were chosen because they were auction winners for government tenders for external information system services.

The Delphi study took several months to complete. The five selected service providers that provide information system services to government agencies were invited, including 15 participants [P1-SP, P2-SP, P3-SP,...,P15-SP] to participate in the process of the Delphi data collection [4].

The research activities were composed of an adaptive wideband Delphi study and grounded theory analysis. The Delphi approach was used to collect data from participants. Then, the grounded theory approach was used to analyse the Delphi study data. The data collection and analysis consisted of three phases of the grounded Delphi study, as follows and shown in Figure 2:

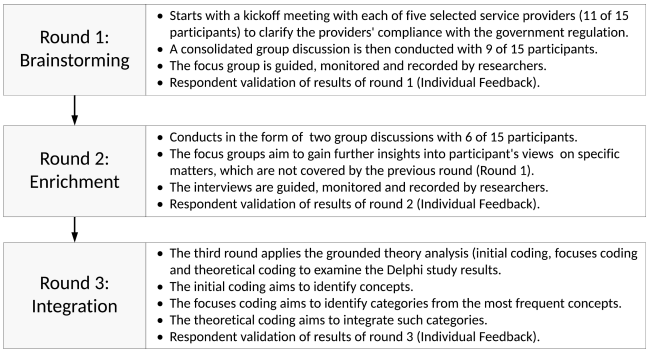

Figure 2: GADM with 15 Provider Participants

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

3.2. Data Analysis

The two sets of empirical data derived from [4][16] were examined using a grounded theory analysis. Validation of research results in [4][16] was carried out through three rounds of the GADM study; the results of each round were sent to each participant, who was asked for feedback and corrections, if any. The results of round 3 [4][16] therefore constitute the validated data used in this paper. Furthermore, the procedure for coding used in the grounded theory analysis in this paper was conducted in three steps: 1) initial coding, 2) focused coding, and 3) theoretical coding [30] to facilitate data analysis in the Delphi study data. This research method enables the researcher to use the Delphi data to develop principles and framework from two empirical studies, with the Government and service provider participants, as shown in Figure 3.

3.3. Initial Coding

After organising the data, an initial coding of the transcribed dataset was conducted to identify concepts. The initial coding's main aim was to discover the principal idea highlighted in each sentence or paragraph.

This initial coding process is similar to the idea of open coding as seen in Glaserian Grounded Theory and Straussian Grounded Theory. The initial coding process breaks the data into concepts

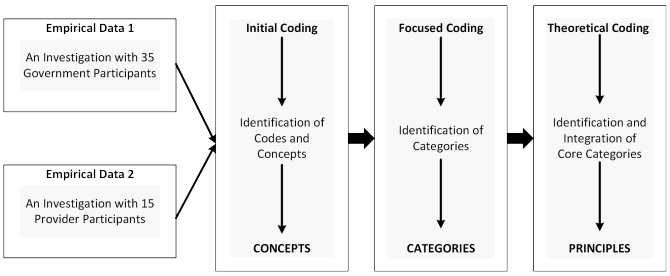

Figure 3: The Research Method - A Grounded Theory Approach

by examining interview or focus group transcripts, word-by-word, line-by-line, incident-by-incident, by sentence or paragraph, or even by the whole documents [30, 35]. Such a process extracts useful sentences or statements and identifies topics of interest, called 'key-point coding.' Organising these initial codes into more complex conceptual codes occurs in focused coding, as shown in Table 1.

Table 1: Examples of the coded data that emerged from the data

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

3.4. Focused Coding

Focused coding follows on from initial coding. The focused coding process was conducted to identify and select categories from the most consistent or significant codes and using them to categorise specific codes.

This coding process is similar to selective coding, based on Glaserian Grounded Theory [36], which focuses on generating codes around identified core variables [35]. The focus coding process is similar to the axial coding step described in Straussian Grounded Theory [37], which involves identifying relationships between categories and subcategories and to each other before being tested against the data [35].

In Charmaz's Grounded Theory [30], the focused coding process allows researchers to select categories from the most common or essential codes [35]. In other words, this coding process begins to select categories from amongst topics of interest and finds relationships among these initial codes (e.g., the most frequent or important codes) [30, 37].

3.5. Theoretical Coding

In the final step, theoretical coding was performed to specify the relationships between core categories to incorporate them into a cohesive framework. All the emerged codes, concepts, categories were compiled to derive principles.

Theoretical coding is at the heart of theory development or theoretical integration [38, 30]. In Glaserian Grounded Theory [36], the theoretical coding aims to identify the conceptual relationships between the substantive codes, thus informing the development of a hypothesis [35].

Similarly, Straussian Grounded Theory [37] discusses a theoretical integration within the process of selective coding, which aims to identify a core category that links all significant categories [35]. Although Straussian Grounded Theory [37] is required to determine a central category, Charmaz's Grounded Theory does not need the choice of core concepts [30].

Once the categories are identified, this step establishes the relationship between the categories to integrate them into a cohesive theory [30]. Overall, this paper uses the grounded theory primarily for data analysis. The outcomes of the grounded theory analysis are elements of the proposed principles or a framework.

The Oxford Dictionary defines a principle as '*a fundamental truth or proposition that serves as the foundation for a system of belief or behaviour or a chain of reasoning*.' In this paper, such a principle contains two or more main categories that are connected using linking words to form a meaningful statement [31]. From this, a framework can be defined as a coherent group of principles. In other words, such principles are the building blocks of developing a TDSLA capability framework. Figure 2 shows the complete list of concepts and categories that emerged from the grounded theory approach.

For the latter step, to validate the grounded theory of this paper, an iterative process of definition and validation of principles and framework were conducted by using the participants' feedback. Further, a minimum agreement of 70% from the participants must be reached to support validation of the principles and framework [32].

4. Framework

This paper aims to develop principles as foundations for a TDSLA capability framework from work on the Indonesian Government's data confidentiality requirements. A qualitative method using grounded theory analysis was chosen to propose principles as foundations for the proposed framework [39]. In this study, the application of grounded theory aims to generate principles and framework rather than use or validate existing framework [40]. The grounded theory approach has become a well-established research methodology by which new frameworks can be uncovered by data collection activities, coding, and categorisation, followed by several comparative and theoretical analyses of findings [28, 29, 30, 34, 32, 33].

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

Data collection from GADM with 25 Government participants and GADM with 15 provider participants was analysed to identify categories and relationships among categories. Therefore, the chosen grounded theory approach is used to develop principles and uncover a TDSLA capability framework.

The framework presented in Figure 4 consists of several categories, depicted in five main categories as proposed principles, as follows:

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

Figure 4 shows that each box represents a core or main category, which can serve as a principle. Each main category consists of an identified set of subcategories. This section begins from the perspective of what to protect to explain the main categories of the framework and their relationships.

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

Moreover, formulating discrete security assurance levels is determined relative to the interplay of data classification levels, data confidentiality risks, SLA data confidentiality requirements, and data confidentiality capabilities. Finally, selecting an appropriate level of security assurance can be incorporated into an SLA. In other words, central to the proposed framework is discrete security assurance levels that can be incorporated into a service level agreement. Formulating discrete security assurance levels are correlated with the main categories of classifying government data, identifying data confidentiality risks, defining SLA data confidentiality requirements, and provisioning data confidentiality capabilities.

Each level of security assurance is distinct from another and offers an increase in the protection against a broader class of threats than the previous level. Thus, the developed framework can help deal with dynamic threats in increasingly global computing environments.

In the following subsection, principles are formulated from the Delphi study data and defined using the main categories and their associations. Each section begins with a box that enables the source from each principle to be tracked through the analysis used in this paper. The core categories are derived from interpretations of insights from participants. All of such principles are novel and direct insights from this study. Furthermore, the checklist **(V)** for each SAL (Security Assurance Level) was derived from interpretations of insights from participants. The amount of data that is processed, transmitted, and stored affects the level of security assurance.

4.1. Classifying Government Data

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

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

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

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

> " *Classifying data is necessary to define in the first place. Also, we need to understand whom the information owner allowed access*"—(P5-SP).

> " *Each ministry should classify its data as public, restricted, secret, and top secret. But, the classification of confidential data in Ministry A may be different classification with the Ministry B*"—(P19-GOV).

While Article 17 of the Indonesian Law on Public Information Transparency number 14 of 2008 and the Regulation Number 17 of 2011 concerning Government Security Classifications and

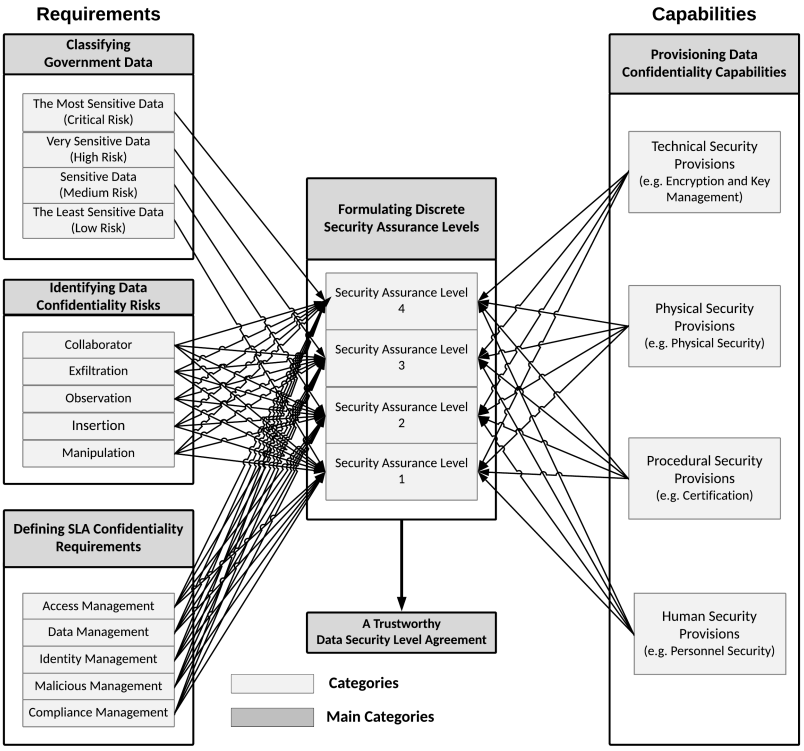

Figure 4: A Trustworthy Data Security Level Agreement (TDSLA) Capability Framework

Table 2: Classifying Government Data

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

Archives cover levels of government data classification, participants reported that there was a need for the Government to formulate and classify data confidentiality requirements for each data classification and risk level.

Law Number 14 of 2008 defines public sector data into three categories of data classification: 1) public; restricted; and secret. Additionally, Regulation Number 17 of 2011 outlines government security classifications into four levels: 1) public; 2) restricted; 3) secret; and 4) top secret. However, both law and regulation do not define an appropriate level of protection for each data classification. For example, each category should include information about security requirements with rules for processing, transmitting, and storing sensitive data.

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

Principle 1

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

4.2. Identifying Data Confidentiality Risks

Identifying data confidentiality risks was defined in the grounded theory analysis as a process in which government agencies perceive confidentiality threats to sensitive government data against unauthorised access. Participants reported that three threat actors determined a risk perception:

- caused by a local adversary (e.g., a customer);
- caused by a service provider (e.g., a cloud provider); and
- caused by a global adversary (e.g., a powerful nation-state).

Overall, the participants' statements indicated that identifying data confidentiality risks was associated with the categories of

Table 3: Identifying Data Confidentiality Risks

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

collaborator, exfiltration, observation, insertion, and manipulation, as shown in Table 2.

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

> "*Regarding key management, our customer can hold the encryption keys, even though the encryption process has been created on the provider side*"—(P1-SP).

> "*Security threats and attacks can come from inside government networks. For example, our observation discovered botnets keep sending out the data from the government networks*"—(P13-GOV).

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

Based on the Delphi study data, the process of identifying and specifying a security-threat environment for each data classification and risk level is linked to the process of formulating discrete levels of security assurance. It is noted that an appropriate level of security assurance required for mitigating each type of threat was derived from interpretations of insights from participants, as shown in Table 3.

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

Principle 2

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

4.3. Defining SLA Data Confidentiality Requirements

Defining government SLA data confidentiality requirements was defined in the grounded theory analysis as a process in which government agencies attempt to formulate and classify the Government's data confidentiality requirements in SLA contexts. Based on the Delphi study data, SLA data confidentiality requirements are in line with the categories of access management, data management, identity management, malicious management, compliance management. Hence, four discrete security assurance levels can be specified using 23 data confidentiality requirements, which were derived from interpretations of insights from participants, as shown in Table 4.

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

> "*We need to establish secure government networks with a single gateway, so if there is a leak, we can know from which point*"—(P1-GOV).

> "*The Government should not allow sensitive government data to be stored in other countries without a strong authentication*"—(P3-GOV).

Many participants highlighted that data confidentiality requirements were necessary for formulating and classifying discrete security assurance levels. There is a relationship between SLA data confidentiality requirements and security assurance levels. However, the fact that few previous studies attempt to investigate government SLA data confidentiality requirements. On top of that, the findings of this study indicate the importance of incorporating discrete security assurance levels in the formulation of SLAs as a means of assurance approach used to verify the security of information system services.

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

Further, security-related SLAs are needed to address the Government's concerns regarding the confidentiality of sensitive government data with a business model of service provisioning. The deployment of external information system services (e.g.,

Table 4: Defining SLA Data Confidentiality Requirements

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

government cloud services) will apply to security and requires new definitions of SLAs for security-relevant requirements. To this end, this study proposes the following principle.

Principle 3

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

4.4. Provisioning Data Confidentiality Capabilities

Providing the required data confidentiality capabilities was defined in the grounded theory analysis as a process in which service providers attempt to provide appropriate capabilities based on the security assurance level. Providing the required capabilities for each level is correlated with the concepts of technical provisions, physical provisions, procedural provisions, and human provisions. It is noted that each security assurance level can include the technical, physical, procedure, and human security provisions, as shown in Table 5.

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

Participants highlighted the importance of trust in and trustworthiness of government supply chains. The majority of participants stated that trust could be achieved by looking at service provider capabilities and qualifications, such as whether service providers have certain types of technical security provisions (e.g., data encryption, data loss prevention, and trusted computing). Additionally, participants stated that the Government usually validated service provider qualifications using certification and accreditation schemes. For example, P6 reported the following statements.

Table 5: Provisioning Data Confidentiality Capabilities

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

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

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

Based on findings here, provisioning data confidentiality capabilities should be a part of the concept of formulating discrete security assurance levels. However, the notion of discrete security assurance levels as the quality of protection has not been extensively discussed in the literature. Also, few studies [7] explicitly link security to SLA capabilities.

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

Principle 4

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

4.5. Formulating Discrete Security Assurance Levels

Formulating discrete security assurance levels was defined through the Delphi study data as a process in which government agencies select an appropriate protection level to determine

the level of security for services that suit government security needs, as shown in Table 5. In this study, formulating discrete security assurance levels is correlated with the main categories of classifying government data, identifying data confidentiality risks, defining SLA data confidentiality requirements, and provisioning data confidentiality capabilities that emerged from the Delphi study data. The participants' statements indicate that there is an association between security assurance levels and SLAs.

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

> "*So far, existing SLAs have focused primarily on availability, while government agencies do not demand SLAs for confidentiality and integrity due to lack of awareness*"—(P31-GOV).

> "*In general, information security-related SLAs do not exist at all. Perhaps, characteristics of services should be defined first because each service has different security features and attributes*"—(P1-SP).

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

The notion of SLAs found in the literature is used to formulate the obligations of a service provider to deliver the agreed service according to a set of government's requirements [7]. However, many SLA provisions contain the quality of services (QoS) attributes regarding system availability and performance aspects [7] in which such QoS services typically do not include data security provisions such as data confidentiality. These findings indicate that formulating discrete security assurance levels is associated with the concepts of classifying government data, identifying data confidentiality risks, defining SLA data confidentiality requirements, and provisioning data confidentiality capabilities.

A pivotal inspiration to formulating discrete security assurance levels that can be incorporated into an SLA is drawn from the NIST Electronic Authentication Guideline SP800-63 [41] and the International Society of Automation (ISA99) on security for industrial automation and control systems [42]. Such approaches relate to four levels of assurance. Level 1 is the lowest assurance level (the least resistant to threats). Level 4 is the highest (the most resistant to threats). Each security assurance level consists of confidentiality considerations of principle 1, principle 2, principle 3, and principle 4, as shown in Table 6. Data confidentiality considerations presented at each level combine well with statements from the participants of this study. Notably, each security assurance level can be adjusted to cope with the increasing sophistication of the threat environment.

Further, the importance of distinct technical requirements in each discrete security assurance level is also underlined in other studies [41][42][43][27]. Discrete security assurance levels play an essential role in supporting the definition and incorporation of the Government's data confidentiality requirements into an SLA. Therefore, this implies the following principle.

Principle 5

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

5. Validation of the Framework

This paper uses four approaches for validating foundations for a TDSLA capability framework: 1) reflection on related works; 2) testimonial validity; 3) use cases; and 4) applications of transferability.

5.1. Reflection on related Frameworks

The SPECS (Secure Provisioning of Cloud Services based on SLA management) framework conducted by European communities [13] is one of the contributions to the field. As part of their research, SPECS has proposed an open-source framework to offer security-as-a-service by relying on the notion of security criteria specified in SLAs. The SPECS framework addresses cloud service providers and cloud service customers to provide techniques and tools for enabling negotiation, monitoring, and enforcement of security criteria in cloud SLAs. SPECS also offers tools to help cloud service providers and cloud service customers to verify the security assurance through Security SLAs, which are based on standard security controls, such as CSA Cloud Control Matrix, NIST 800-53 Rev.4, and ISO/IEC 27017 – Information security controls for cloud services.

Compared to the SPECS framework, the TDSLA capability framework that emerged from the Delphi study data aims at certifying levels of security for services by incorporating discrete security assurance levels into SLA contexts. In a similar vein to SPECS, security assurance levels are linked to customers' security requirements and service providers' security capabilities. However, the four discrete levels of increasing security assurance allow for cost-effective solutions appropriate for various information system services that process, store or transmit government data. The framework enables government agencies

Table 6: Formulating Discrete Security Assurance Levels

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

to select an appropriate security assurance level based on the data classification and risk level. Government agencies can use the framework to procure and use cloud-based services by determining an appropriate level of protection according to their security needs and requirements.

Similarly, the multi-cloud secure applications (MUSA) framework is developed to support the security-intelligent lifecycle management of distributed multi-cloud applications [14]. MUSA extends the Security SLA of SPECS with additional features. The MUSA framework is developed to detect violations of such composite Security SLA. MUSA offers an integrated tool to monitor and enforce the secure behaviour stated in the Security SLA of the multi-cloud application [44].

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

Likewise, SLA-ready is developed to provide a reference model for developing cloud SLAs and a set of digital services to support cloud service customers in the use of SLAs [15]. The reference model is based on standard specific requirements, including functional, non-functional, security, data protection, legal, and business requirements. The SLA model uses security controls from the CSA Cloud Control Matrix and the ISO/IEC 19086 standard on Cloud Computing SLA Framework to specify security and privacy policies in SLAs. The TSDLA framework developed from this research purposely does not aim to incorporate security controls into contracts or SLAs. However, this study formulates and classifies security controls into discrete security assurance levels to protect government data against unauthorised access.

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

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

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

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

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

Therefore, these are the reasons to construct better assurance mechanisms in service provision that give government agencies as much transparency and confidence as possible that any sensitive government data transferred to service providers is processed, stored, and transmitted securely. Also, the framework is easy to use without deep expertise. Service providers are required to provide evidence that the service they are offering can potentially demonstrate agreed security assurance levels. A government tender could review whether the service provider's capabilities align with technical requirements for the required level of assurance.

5.2. Testimonial Validity

Testimonial validity refers to the accuracy of the researcher's interpretations by checking whether the principles and framework that emerged from the Delphi data are convincing to participants from the Government and service providers [45, 46, 47]. In this study, the researcher provided the opportunity for the participants to comment on the principles and framework obtained from the Delphi data. All 50 participants were invited to participate in the validation; 19 participants responded. The principles and framework were assessed by the participants using a five-Likert scale questionnaire and open-ended questions. An iterative process of definition and validation of principles and framework was conducted using the participants' feedback. The aim is not to estimate the distribution of participants' opinions but to have early information about the principles and framework's expected completeness and usefulness.

The overall validation is positive; most participants agree with the principles and framework that emerged from the data. The positive opinions of participants may be motivated by a desire to finish the feedback quickly or be kind to the researcher. However, the critical feedback is also beneficial, especially if the participant can indicate which elements and framework would not be useful in real-world contexts. These factors were addressed by quantitatively assessing feedback. In this paper, the evaluation feedback is aimed at providing a minimum of 70% agreement from the participants to support validation of principles and framework [32]. Thereby, participants confirmed the correctness and practicability of the findings that emerged in the research, even though the summarised results did not necessarily reflect every single opinion and statement.

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

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

needs. The findings identify consistencies with the participants' expectations.

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

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

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

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

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

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

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

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

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

In summary, 19 participants were asked to evaluate the framework for its completeness and usefulness. There were a few inconsistencies between the principles and framework and the participants' perceptions regarding completeness. All of the participants identify the usefulness of the framework. While there was agreement about the usefulness of the framework, some suggestions were made to expand the scope of the framework. For example, how the framework can support government procurement for services that process, transmit or store sensitive government data.

5.3. Using the Framework to capture real-world cases

We apply it to three use cases to demonstrate the framework's use in assessing various metrics in different scenarios. Some examples of the security assurance levels are presented in the context of a government cloud in the following requirements: access management, data management, and malicious management.

Access Management

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

It is acknowledged that cloud-based services remove the concept of the 'air-gap' approach, such as network virtualisation,

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

server virtualisation, and storage virtualisation [48, 49]. However, data and network isolation need to be considered carefully to achieve as much of a security requirement as possible in SLAs. For example, most virtual machines run on the same physical hardware, leading to sharing the underlying infrastructure with untrusted customers. However, common access control and security policies are insufficient to ensure isolation in cloud data centre services. Thus, isolated networks at Level 3 may provide an acceptable level of protection against unauthorised data disclosure from trusted to untrusted cloud-based services. Overall, **Security Assurance Level 3** may be suitable for this case. It is expected that this level of security precautions can mitigate the threats at least increase the efforts required to access sensitive government data.

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

Data Management

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

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

Of course, key management is critical and challenging in a cloud environment [50]. Cloud-based services can provide a secure connection using TLS or SSH. Like traditional data centres, cloud data centres also can store application data in an encrypted form. If the Government requires high data confidentiality requirements, cloud service providers can provide end-to-end encryption. In this case, cloud service providers must provide evidence to demonstrate that they do not have access to the encryption keys or they would not be able to hold those keys over unauthorised entities. Thus, the need for third-party vendor protection requirements would be required to be built into contracts or SLAs, as most services or applications store data in cloud data centres. One also needs to look at the entire data supply chain when data is stored in multiple locations and in what country the data is stored. Overall, in the context of a government cloud, the specified levels of assurance will be appropriate at **Security Assurance Level 3**.

Malicious Management

It is necessary to include physical security attributes in the formulation of security-related SLAs through security assurance levels. In practice, many cloud service providers claim that they have 24 x 7 x 365 services on-site physical security to protect against unauthorised entry, which can be checked through security audits to help build the trust and confidence between a customer and a service provider [51]. Physical security controls can include security guards, physical access control devices (e.g., locks), physical intrusion alarms, and surveillance types of equipment (e.g., CCTV) [52].

Further, the physical location of cloud data centres has been highlighted as a significant concern since the Edward Snowden revelations in 2013. Although data security depends not only on its geographical location, many governments cannot store citizen's data under other jurisdictions. For instance, according to Article 17 of the Indonesian Government Regulation on the Operation of Electronic Systems and Transactions, Number 82 of 2012, mentioning that Electronic System Operators have obligations to locate data centres within the borders of national jurisdictions, especially for law enforcement and protecting citizen's data against force majeure (e.g., earthquakes, floods, and wars)[53]. In particular, localised data centres may help to get access and apply digital forensics to cloud-based services for law enforcement. Therefore, it is essential to include the physical location of data centres in the formulation of security-related SLAs when using cloud-based services provided by external service providers, especially for processing, transmitting, and storing sensitive government data. In the context of a government cloud in general, this corresponds to **Security Assurance Level 3**.

5.4. Applications of Transferability

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

The UK G-Cloud Framework

The UK-Government Cloud (G-Cloud) is one of the most extensive cloud government procurement frameworks. The G-Cloud consists of framework agreements with cloud service providers and the digital marketplace, allowing government and public sector organisations to search for cloud services listed in the G-Cloud Framework. The UK Government agencies can procure and purchase cloud services listed on the digital marketplace without calling for a full tender process [54].

Within the existing G-Cloud framework, the self-assertion approach developed is far more practical [55]. In the same vein, the use of the TDSLA capability framework is feasible in this context. Cloud service providers must go through a set of discrete security assurance levels, which are determined based on the service they are offering, and provide self-assertion of compliance.

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

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

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

The US FedRAMP Framework

The Federal Risk and Authorization Management Program (FedRAMP) [56][57] is the US government framework that carries out a standard approach to the security assessment, authorisation, and continuous monitoring for cloud services. The framework requires cloud service providers interested in offering their services to the US government to receive an independent security assessment conducted by a third-party assessment organisation to ensure that authorisations are compliant with the Federal Information Security Management Act (FISMA).

However, such a process is particularly complex where cloud service providers rely on an independent third-party assessment organisation. Additionally, obtaining such certification and accreditation is a bureaucratic process. There is a need for further time and costs for service providers, resulting in increased prices. The application of FedRAMP also requires significantly more effort and pre-established security infrastructure [57].

On top of that, the self-assertion approach developed under the TDSLA capability framework seems to be more practical and feasible in this context. Cloud service providers interested in providing cloud services to US federal government agencies

are required to go through a set of discrete assurance levels determined based on the service they are offering and provide self-assertion of compliance.

Furthermore, service level agreements are intended to examine a service provider's capabilities to meet the government's data security requirements and agree on the required and provided a level of security assurance between parties. The simplification of the framework proposes four discrete security assurance levels that help steer federal agencies towards the compliant adoption of cloud services. The formulation of the data classification scheme applied in each assurance level has helped make it more transparent how sensitive government data is to be processed, transmitted, or stored.

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

6. Discussion

The principles and framework formulated during this study are summarised in Table 7 by giving details on five related aspects: 1) understanding based on findings and literature; 2) proof of quotations (random selection); 3) reflection against related work; 4) agreement to support validation on the derived principles and framework; and 5) position of applicability.

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

Evaluating a security service requires identifying the customer's security needs and assessing the capabilities of service providers that offer services. The proposed framework aids customers in both processes through two key components: discrete security assurance levels and service level agreements. A discrete security assurance level defines a standard set of data security requirements for a specific type of service. The value of the discrete security assurance levels comes from the idea that any objective observer will agree about what level is achieved by a particular service. In other words, it is necessary to have clarity about what characterises the different levels for each data classification and threat environment. Ideally, customer expectations should be transparent in legal language. Hence, these levels of agreement can form the basis for constructing a legal language in contracts or SLAs.

Further, by listing the required level of assurance for service families, the proposed framework allows a service provider to state conformity to a relevant level of security assurance, which is determined based on the services they are offering to government agencies. For example, a service provider intended to process, transmit and store general personal data (e.g., name, date of birth, national identity) must go through security assurance level 2 (SAL2). On the other hand, if the service offered by a service provider process, transmit and store specific personal data (e.g., Biometric), a service provider is required to state conformity to the security assurance level 3 (SAL3) such as multi-factor authentication and mutual authentication of a user and cloud service provider are required [58, 59]. In other words, the service is tested against a specific level of security assurance, providing reliable verification of the security capabilities of the service. Since the security of information system services can be linked to a particular security assurance level, customers can assess a list of security requirements and features by examining the details of a relevant level of security assurance. Also, customers can determine the service's ability to meet their security needs and compare the security capabilities of any other services.

Based on the findings, the TDSLA capability framework is developed to incorporate the Government's data confidentiality requirements into an SLA. One benefit of using such a framework is that the ability of the framework to include discrete security assurance levels, which are determined based on the service they are offering. This framework has allowed service providers to deliver an appropriate level of security assurance in the provision of procured services. Moreover, this leads to a simple means of incorporating the Government's data confidentiality requirements into an SLA between government agencies and service providers by allowing government agencies that do not have the technical knowledge to specify government security needs merely. For example, a government tender could entail security assurance level 3 (SAL3) for processing biometrics data. At the same time, service providers who are keen to provide such services must satisfy the required level of assurance.

An essential decision in the formulation and classification of the Government's data confidentiality requirements into discrete security assurance levels was the need to ensure the simplicity and clarity of applying the proposed framework. The aim is to provide sufficient practical knowledge to novice staff without requiring them to learn how to classify data confidentiality requirements and capabilities according to types of threats or vulnerabilities. Therefore, government agencies that possess deficiencies in identifying the required Government's data confi-

dentiality requirements and capabilities can select an appropriate service provider that offers the level of security assurance required to protect sensitive government data, thereby improving the overall quality of government procurement of external information system services.

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

6.1. Challenges for the framework

There are a few challenges in the application of the concept of a TDSLA capability framework. One of the main concerns about the framework is its applicability in the real world and the need for further elaboration using a wider range of information system services. Further work should examine acceptable discrete security assurance levels in different service provisioning scenarios and consider how the TDSLA framework would apply to each of these scenarios.

There are two main questions for which the concept of a TDSLA capability framework may be applied in various service scenarios. Firstly, incorporating discrete security assurance levels into the context of SLA would need to be expressed. Secondly, how to evaluate whether the use of discrete security assurance levels required is in line with customer's requirements and service provider's capabilities. The means of compliance checking are not worth much attention until clear definitions of discrete levels of security assurance are provided. As such, it is necessary to formulate and classify distinct technical requirements for each security assurance level.

Another challenge is in characterising data confidentiality risks within each discrete security assurance level, especially when attempting to include specific risks or threat models into SLA contexts. Such threats are guaranteed to be mitigated based on the discrete level of security assurance required. For example, in the case of purchasing insurance, the degree of exposure to a particular type of risks or threats can be predicted and guaranteed with pricing levels [9]. However, it is hard to estimate the costs of maintaining security capabilities in the case of assurance services. Security risks or threats identified for each discrete level of security assurance tend to behave unpredictably from time to time.

Further, an additional difficulty is how to classify data confidentiality capabilities according to threats, especially when government agencies decide to procure external information system services to process, store, or transmit sensitive data on behalf of the Government. For instance, SLAs can be formulated based on specific threats and technical 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 with the incorporation of appropriate discrete levels of security assurance into SLA contexts. These questions have been identified as future work.

A final criticism can be directed to the methodology used in the research, including research design, setting and participant, data collection technique, and data analysis. Despite the measures taken to validate and generalise findings, the ability to make generalisations based on this study is limited by the number of participants from a single country. Additional cases with more participants from other countries might present more fundamental principles, with more capacity for generalisation. Overall, these limitations provide opportunities for future research to build on the findings of this study.

7. Conclusion

This paper has investigated a future assurance approach for service provisioning based on discrete security assurance levels incorporated into SLA contexts. The Indonesian Government's data confidentiality requirements were used to develop foundations for a TDSLA capability framework. This resulted in an initial TDSLA capability framework. However, it is anticipated that the concept of a TDSLA capability framework can be broader to other data security requirements. In other words, four discrete levels of security assurance can be extended and elaborate on other security properties of data integrity and data availability.

The key inspiration and reference point for building a TDSLA capability framework is the CC certification process. CC aids in building trust through two main components: protection profiles; and evaluation assurance levels (EALs). In comparison, developing foundations for a TDSLA capability framework consists of two main parts: discrete security assurance levels; and service level agreements.

A discrete level of security assurance defines a standard set of data security requirements for a specific type of threat and data classification level. The technical, procedural, and human elements of information security are necessary to achieve the required level of security assurance. Each level of assurance is distinct from another, depending on data classification and threat model. In addition to discrete security assurance levels, the use of service level agreements is intended to examine the service provider's capabilities to meet the customer's data security requirements and to agree with the required and provided a level of security assurance among contracting parties.

Therefore, these are the reasons to construct better assurance mechanisms in service provision that gives government agencies transparency and confidence as any sensitive government data transferred to service providers is processed, transmitted, and stored securely against unauthorised access. In other words, the CC aims to certify levels of security for products. In contrast, the

Table 7: Understanding, Proof, Agreement, Reflection and Position

	A TDSLA Capability Framework	Principle #1: Classifying Government Data	Principle #2: Identifying Confidentiality Risks
Understanding based on findings and literature	Incorporating standard security controls like NIST 800-53 and ISO/IEC 27002 into SLAs constitute security-related SLAs. However, these approaches do not incorporate data confidentiality requirements into SLAs according to data classification and threat environment.	Any parties who work with the Government have to ensure such sensitive data is appropriately protected under the Government's requirements. However, there is little recognition of SLAs' level of assurance according to data classification and threat environment.	There is little recognition of incorporating data confidentiality risks, which are mitigated by each discrete level of security assurance. A service provider may conduct a risk assessment concerning a distinctive level of security assurance. Each level protects against different threats.
Proof Quotation for the principles and framework presented in figure 7.2 (random selection)	"*Existing SLAs have focused primarily on availability, while customers do not demand SLAs for confidentiality and integrity due to lack of awareness* (P31-GOV)" "*In general, information security-related SLAs do not exist at all. Perhaps, characteristics of services should be defined first because each service has different security features and attributes*" (P1-SP)	"*Regarding data, classifying data is necessary to define in the first place. Also, we need to understand whom the information owner allowed access*" (P5-SP) "*Each ministry should classify its data as public, regulated, restricted, secret, and top secret. However, the classification of confidential data in Ministry A may be different classification with ministry B*" (P19-GOV)	"*Regarding key management, our customer can hold the encryption keys, even though the encryption process has been created at the provider side*" (P1-SP) "*Actually, threats and attacks can come from inside government networks, such as our observation discovered botnets keep sending out the data*" (P13-GOV)
Reflection against related works	The SPECS Framework [13], The MUSA framework [14] and SLA-Ready [15]. Overall, SLAs' importance on discrete levels of assurance is still not fully considered when service providers are handling sensitive data. The key inspiration and reference point for building a TDSLA capability framework is the CC certification process.	Data classification for cloud readiness [60], Government Security Classification [61]. The existing literature does not focus on the data classification level that can be expressed in SLA contexts. There may be other data management constraints over sensitive government data (e.g. data protection, national security and health regulation)	Assurance levels against threats [27, 41, 43], Risk Management [14], Threat Analysis [14]. In short, the existing literature does not identify the linkage between threat mitigation and an appropriate level of security assurance incorporated into SLA contexts. Each level is expected to have different capabilities against threats.
Agreement to support validation	100%	94.7%	94.7%
Position of applicability	The framework can be applied to a specific context such as Amazon Web Services - UK Government Cloud (AWS-G Cloud) and AWS-The Federal Risk and Authorization Management Program (AWS-FedRAMP) to show the applicability of the framework.	Classifying government data can be expressed in the formulation of assurance-based SLA. Thus, this principle can encourage lucidity and characterise certain levels of protection ranging from the lowest level of assurance to the highest level.	This principle can help to quantify a defined risk tolerance level for each level incorporated into SLAs. Identifying perceived confidentiality risks is essential to avoid ambiguity about which appropriate level of assurance a customer requires.

TDSLA capability framework aims to certify levels of security for services.

This study was the first of its kind in Indonesia to take a holistic assurance approach to service provisioning in government procurement by engaging all three types of entities: permanent government officials, government consultants, and service providers. It has provided a much-needed evidence base to support the more widespread implementation of the TDSLA capability framework. In doing so, this paper contributes to service provision, with a focus on the Indonesian Government. Finally, this research endeavour hopes to pave the way for further investigations of better security assurance services in global computing environments.

While this paper has demonstrated the potential of incorporating the Government's data confidentiality requirements into SLA-based discrete security assurance levels, many opportunities for extending the scope of this study remain. This section presents some of these directions. The first possible direction of research is to elaborate more on classifying government data. The existing laws and government regulations do not give detailed security 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).

The second possible extension is to enrich the expressiveness of threat model statements. Without an actual threat model, it is difficult to classify a threat to a particular level of security assurance. The proposed threat models for each level of security assurance 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 security assurance.

Finally, the findings of this study indicate that discrete levels of security assurance play an essential role in supporting the definition and inclusion of the Government's data confidentiality requirements into an SLA. The discrete security assurance levels presented are evidently in need of further elaboration. It is expected that the discrete levels of security assurance can be adjusted to cope with the increasing sophistication of the threat environment. It is anticipated that each discrete level of security assurance offers an increase in the range of threats addressed over the previous level. These four increasing levels of security assurance allow cost-effective solutions that are appropriate for various applications and domains.

References

[1] Y. Nugraha, I. Brown, A. S. Sastrosubroto, An adaptive wideband delphi method to study state cyber-defence requirements, IEEE Transactions on Emerging Topics in Computing 4 (2016) 47–59. doi:10.1109/TETC.2015.2389661.

[2] M. Anisetti, C. Ardagna, E. Damiani, F. Saonara, A Test-based Security Certification Scheme for Web Services, Proceedings of ACM Trans. Web 7 (2013) 5:1–5:41. URL: http://doi.acm.org/10.1145/2460383.2460384. doi:10.1145/2460383.2460384.

[3] R. Böhme, Security Audits Revisited, Springer Berlin Heidelberg, 2012.

	Principle #3: Defining SLA Data Confidentiality Requirements	Principle #4: Provisioning Data Confidentiality Capabilities	Principle #5: Formulating Discrete Security Assurance Levels
Understanding based on findings and literature	Defining government SLA data confidentiality requirements is necessary to delineate the quality of protection or an appropriate discrete security assurance expressed in SLAs. This context raises questions on whether data confidentiality can be adequately expressed in SLA contexts.	The quality of protection is measured according to the confidentiality capabilities of a service provider to deliver the agreed service based on a set of data co h 4ionfidentiality requirements. Provisioning data confidentiality capabilities are different for each level of security protection.	There is little recognition of discrete security assurance levels expressed in SLAs. Whereas there is a need to incorporate specific security clauses into an SLA-based discrete security assurance level that defines a standard set of data security requirements against unauthorised access.
Proof Quotation for our principles and the framework presented in figure 7.2 (random selection)	"*we have to create a single entry point for government secure communications and networks so that should there is any leak, we can easily find it out*"(P1-GOV). "*the Government should not allow any sensitive government data to be stored and hosted in other countries without extra security controls taken place, such as a strong password*" (P3-GOV).	"the highest level, there is a tamper-proof mechanism, if there is a rigorous attempt to obtain sensitive data; this can perform active zeroisation" (P6-GOV) "*we can encrypt data in transit, using VPN, SSL, and IPSec. We can use storage encryption and DLP for protecting data at rest; we can provide a hardware security module for customers*" (P4-GOV)	"*Existing SLAs have focused primarily on availability, while customers do not demand SLAs for confidentiality and integrity due to lack of awareness*" (P31-GOV) "*Security-related SLAs does not exist at all. Perhaps, characteristics of services should be defined first because each service has different security features and attributes*" (P1-GOV)
Reflection against related works	UK Cloud Security Principles [55], Security Requirements for protecting the confidentiality of CUI [62]. Based on the literature, we deepen the understanding by providing insights into government SLA data confidentiality requirements investigated in this study.	Introduction to AWS Security capabilities [63], Meaningful Security SLAs [10], Building Security SLAs [12]. Building upon the knowledge of previous studies, we deepen the understanding of incorporating a service provider's data confidentiality capabilities into SLA contexts.	Security SLAs for Federated Cloud Services [7], Quality of Security Services [64], Security SLAs [11], NISTSP800-63 [41], ISA99 [42]. There appears to be an insufficient investigation into incorporating the Government's data confidentiality requirements in SLAs.
Agreement to support validation	84.2%	89.5%	100%
Position of applicability	This principle has significant implications for providing useful guideline when formulating discrete levels of assurance. Each level has a different level of SLA confidentiality requirements.	This principle is necessary for guiding for delivering the required confidentiality capabilities for each level of assurance, and it is beneficial to incorporate such provisions into SLA contexts.	This principle can be used to formulate SLA-based discrete levels of assurance that play an essential role in supporting the definition and enforcement of security considerations in SLA contexts.

[4] Y. Nugraha, A. Martin, Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments, 11th IFIP WG 11.11 International Conference on Trust Management, Cham: Springer, 2017, pp. 57–75. doi:10.1007/978-3-319-59171-1_6.

[5] R. Anderson, Security engineering, John Wiley & Sons, 2008.

[6] B. Duncan, M. Whittington, Compliance with Standards, Assurance and Audit: Does This Equal Security?, in: Proceedings of the 7th International Conference on Security of Information and Networks, ACM, 2014, pp. 77:77–77:84. URL: http://doi.acm.org/10.1145/2659651.2659711. doi:10.1145/2659651.2659711.

[7] K. Bernsmed, M. G. Jaatun, P. H. Meland, A. Undheim, Security SLAs for Federated Cloud Services, in: Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES), IEEE, 2011, pp. 202–209.

[8] M. Jaatun, K. Bernsmed, A. Undheim, Security SLAs–an idea whose time has come?, in: Multidisciplinary Research and Practice for Information Systems: IFIP WG 8.4, 8.9/TC 5 International Cross-Domain Conference and Workshop on Availability, Reliability, and Security, CD-ARES 2012, Prague, Czech Republic, August 20-24, 2012. Proceedings, Springer, 2012, pp. 123–130.

[9] R. Henning, Security Service Level Agreements: Quantifiable Security for the Enterprise?, in: Workshop on New security paradigms, ACM, 1999, pp. 54–60.

[10] B. Monahan, M. Yearworth, Meaningful Security SLAs, HP Labs, Bristol, Tech. Rep (2008).

[11] J. Luna, N. Suri, M. Iorga, A. Karmel, Leveraging the Potential of Cloud Security Service-Level-Agreements through Standards, IEEE Cloud Computing 2 (2015) 32–40.

[12] T. Takahashi, J. Kannisto, J. Harju, S. Heikkinen, B. Silverajan, M. Helenius, S. Matsuo, Tailored Security: Building Nonrepudiable Security Service-Level Agreements, IEEE Vehicular Technology Magazine 8 (2013) 54–62. doi:10.1109/MVT.2013.2269188.

[13] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, Security as a service using an sla-based approach via SPECS, in: IEEE 5th International Conference on Cloud Computing Technology and Science, 2013, pp. 1–6. doi:10.1109/CloudCom.2013.165.

[14] E. Rios, E. Iturbe, L. Orue-Echevarria, M. Rak, V. Casola, Towards self-protective multi-cloud applications: Musa–a holistic framework to support the security-intelligent lifecycle management of multi-cloud applications (2015).

[15] S. Ready, The SLA ready project, 2015. URL: http://www.sla-ready.eu/.

[16] Y. Nugraha, A. Martin, Investigating SLA Confidentiality Requirements: A Holistic Perspective from the Government Agencies, Proceedings of 11th International Conference on Emerging Security Information, Systems and Technologies (2017).

[17] K. Howard, 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.

[18] A. Stellman, J. Greene, Applied Software Project Management, " O'Reilly Media, Inc.", 2005.

[19] T. Päivärinta, S. Pekkola, C. Moe, Grounding Theory from Delphi Studies, in: Proceedings of International Conference on Information Systems, volume 3, Association for Information Systems, 2011, pp. 2022–2035.

[20] M. Turoff, The Design of A Policy Delphi, Technological Forecasting and Social Change 2 (1970) 149–171.

[21] G. Greenwald, E. MacAskill, NSA PRISM Program Taps in to User Data of Apple, Google and Others, *The Guardian: Guardian News and Media*. Available: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, June 2013. Accessed 17 December 2017.

[22] T. Klaus, Security Metrics-Replacing Fear, Uncertainty, and Doubt, Taylor & Francis, 2008.

[23] S. Pfleeger, R. Cunningham, Why measuring security is hard, IEEE Security & Privacy 8 (2010) 46–54.

[24] A. Martin, J. Davies, S. Harris, Towards a Framework for Security in e-Science, in: 2010 IEEE Sixth International Conference on e-Science, 2010, pp. 230–237. doi:10.1109/eScience.2010.19.

[25] S. P. Kaluvuri, M. Bezzi, Y. Roudier, Bringing common criteria certification to web services, in: Proceedings of IEEE Ninth World Congress on Services, 2013, pp. 98–102. doi:10.1109/SERVICES.2013.17.

[26] S. P. Kaluvuri, M. Bezzi, A. Sabetta, Y. Roudier, R. Menicocci, V. Bagini, A. Riccardi, M. Orazi, Applying Common Criteria (CC) to Service Oriented Architectures (SOA), in: ICCC 2012, International Common Criteria Conference, September 18-20, 2012, Paris, France, 2012. URL: http://www.eurecom.fr/publication/3906.

[27] D. Herrmann, Using the Common Criteria for IT Security Evaluation, CRC Press, 2002.

[28] S. McGregor, P. Charters, T. Holliday, F. Roesner, Investigating the Computer Security Practices and Needs of Journalists, in: Proceedings of 24th USENIX Security Symposium (USENIX Security 15), 2015, pp. 399–414.

[29] S. Egelman, S. Jain, R. Portnoff, K. Liao, S. Consolvo, D. Wagner, Are You Ready to Lock?, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 750–761.

[30] K. Charmaz, Constructing grounded theory, Sage, 2014.

[31] D. Dor, Y. Elovici, A Model of the Information Security Investment Decision-Making Process, Computers & Security 63 (2016) 1–13.

[32] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, M. Whitty, Understanding insider threat: a framework for characterising Attacks, in: Proceedings of IEEE Security and Privacy Workshops, 2014, pp. 214–228. doi:10.1109/SPW.2014.38.

[33] M. Lerch, P. Spieth, Innovation Project Portfolio Management: A Qualitative Analysis, IEEE Transactions on Engineering Management 60 (2013) 18–29. doi:10.1109/TEM.2012.2201723.

[34] D. Dor, Y. Elovici, A Model of the Information Security Investment Decision-Making Process, Computers & Security 63 (2016) 1–13.

[35] K.-J. Stol, P. Ralph, B. Fitzgerald, Grounded theory in software engineering research: a critical review and guidelines, in: Proceedings of the 38th International Conference on Software Engineering, ACM, 2016, pp. 120–131.

[36] B. G. Glaser, A. L. Strauss, The Discovery of Grounded Theory: Strategies for Qualitative Research, Transaction publishers, 2009.

[37] J. Corbin, A. Strauss, Grounded Theory Research: Procedures, Canons, and Evaluative Criteria, Qualitative sociology 13 (1990) 3–21.

[38] M. Birks, J. Mills, Grounded Theory: A Practical Guide, Sage, 2015.

[39] B. Glaser, A. Strauss, E. Strutzel, The Discovery of Grounded Theory; Strategies for Qualitative Research., Nursing Research 17 (1968) 364.

[40] K. J. Stol, P. Ralph, B. Fitzgerald, Grounded Theory in Software Engineering Research: A Critical Review and Guidelines, in: 2016 IEEE/ACM 38th International Conference on Software Engineering (ICSE), 2016, pp. 120–131. doi:10.1145/2884781.2884833.

[41] W. Burr, D. Dodson, W. William, Electronic Authentication Guideline, NIST, 2013.

[42] J. Gilsinn, R. Schierholz, Security Assurance Levels: a Vector Approach to Describing Security Requirements, in: Proceedings of the US DHS industrial control systems joint working group (ICSJWG) 2010 Fall Conference, Seattle, USA, 2010.

[43] T. Caddy, FIPS 140-2, in: Encyclopedia of Cryptography and Security, Springer, 2011, pp. 468–471.

[44] B. Crespo, E. Prieto, E. Rios, M. Rak, R. C. S. P. Deussen, P. Samarati, S. K. Braun, T. Lorunser, Research and Innovation Challenges in Data Protection, Security and Privacy in the Cloud, January, 2016.

[45] W. Stiles, Evaluating Qualitative Research, Evidence-Based Mental Health 2 (1999) 99–101.

[46] H. Brink, Validity and Reliability in Qualitative Research, Curationis 16 (1993) 35–38.

[47] I. Fléchais, Designing Secure and Usable Systems, Ph.D. thesis, University College London, 2005.

[48] R. Chaudhary, N. Kumar, S. Zeadally, Network service chaining in fog and cloud computing for the 5g environment: Data management and security challenges, IEEE Communications Magazine 55 (2017) 114–122. doi:10.1109/MCOM.2017.1700102.

[49] R. Chaudhary, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, Optimized big data management across multi-cloud data centers: Software-defined-network-based analysis, IEEE Communications Magazine 56 (2018) 118–126. doi:10.1109/MCOM.2018.1700211.

[50] J. Tsai, N. Lo, A privacy-aware authentication scheme for distributed mobile cloud computing services, IEEE Systems Journal 9 (2015) 805–815. doi:10.1109/JSYST.2014.2322973.

[51] H. Hamilton, An examination of service level agreement attributes that influence cloud computing adoption (2015).

[52] J. T. Force, T. Initiative, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800 (2013) 8–13.

[53] Y. Nugraha, Kautsarina, A. S. Sastrosubroto, Towards Data Sovereignty in Cyberspace, in: 2015 3rd International Conference on Information and Communication Technology (ICoICT), 2015, pp. 465–471. doi:10.1109/ICoICT.2015.7231469.

[54] O. Diez, A. Silva, GovCloud: Using Cloud Computing in Public Organizations, IEEE Technology and Society Magazine 32 (2013) 66–72. doi:10.1109/MTS.2013.2241473.

[55] National Cyber Security Centre, Implementing the Cloud Security Principles, Available: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles, 2016.

[56] L. Taylor, FedRAMP: History and Future Direction, IEEE Cloud Computing 1 (2014) 10–14. doi:10.1109/MCC.2014.54.

[57] U. S. Government, Federal Risk and Authorization Management Program (FedRAMP), Online: https://csrc.nist.gov/csrc/media/events/ispab-february-2012-meeting/documents/feb3_fedramp_ispab.pdf, 2012. Accessed 18 Oct 2017.

[58] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, J. J. P. C. Rodrigues, Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment, IEEE Internet of Things Journal 5 (2018) 4900–4913. doi:10.1109/JIOT.2018.2877690.

[59] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, A. V. Vasilakos, On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services, IEEE Access 5 (2017) 25808–25825. doi:10.1109/ACCESS.2017.2764913.

[60] F. Simorjay, Data Classification for Cloud Readiness, Available Online: https://download.microsoft.com/download/0/A/3/0A3BE969-85C5-4DD2-83B6-366AA71D1FE3/Data-Classification-for-Cloud-Readiness.pdf, 2014. Accessed 18 October 2017.

[61] U. K. Cabinet Office, Government Ssecurity Classifications, Available Online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf, 2014. Accessed 17 December 2017.

[62] R. Ross, P. Viscuso, G. Guissanie, K. Dempsey, M. Riddle, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, NIST Special Publication 800 (2015) 171.

[63] A. W. S. Services, Introduction to AWS Security, Available Online: https://d0.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf, 2015.

[64] C. Irvine, T. Levin, Quality of Security Service, in: Proceedings of the 2000 workshop on New security paradigms, ACM, 2001, pp. 91–99.