Investigating SLA Confidentiality Requirements: A Holistic Perspective for the Government Agencies

Yudhistira Nugraha*†, Andrew Martin*

*Centre for Doctoral Training in Cyber Security
Department of Computer Science, University of Oxford, Oxford, UK
†Directorate of Information Security, Ministry of ICT, Jakarta, Indonesia

Email: {yudhistira.nugraha, andrew.martin}@cs.ox.ac.uk

***Abstract*—Many governments consider the use of remote computing, communications and storage services provided by external service providers to process, store or transmit sensitive government data to increase scalability and decrease costs of maintaining services. The use of assurance approaches based on service level agreement (SLAs) is becoming increasingly important in procuring a wide range of such services from external service providers. However, such existing SLAs are not well-suited to a dynamic cyber threat environment because SLA security requirements (considering data confidentiality) have not been deeply studied by the academic computer security community. Such an understanding of the real needs of government is essential to the formulation of security-related SLAs. This paper seeks to provide such insights, by investigating 35 government participants using Indonesia as case study via a grounded adaptive Delphi study. We found that undeveloped SLA confidentiality requirements can illuminate other administrations to include government's security requirements and security capabilities of the service providers in SLAs when using such external services. Based on our findings, we make recommendations to the government agencies, service providers and researchers for improvement to existing SLA definition and future lines of research.**

***Keywords*–Security, Trust, Assurance, Confidentiality Requirements, Service Level Agreement (SLA), Service Provision**

I. Introduction

In recent decades, many government agencies (GAs) generate, collect, store and share far more sensitive data than private organisations within and with external agencies. In fact, there is evidence that GAs increasingly rely on external service providers (SPs) to operate a wide range of remote computing, communications and storage services (e.g. cloud-based services) on behalf of the government. The relationships with external SPs are usually established through service level agreements (SLAs), which are binding agreements between GAs and external SPs. Such SLAs are mainly focused on the system availability and performance aspects, but overlook data confidentiality and integrity in SLAs.

Several attempts have been made to express security properties in SLAs, such as *Secure Provisioning of Cloud Services based on SLA Management* (SPECS) [1], the *Multi-Cloud Secure Applications* (MUSA) [2], SLA-Ready [3] and SLALOM [4]. However, these frameworks are not widely used in a government context, especially for procuring such remote computing, communications and storage services from external SPs. Yet there has been no detailed investigation of the government SLA confidentiality requirements that can be used in the formulation of security-related SLAs. Although some researchers have carried out extensive research on the development of security-related SLAs [5]–[10], no single study exists that has a clear direction for an understanding of government SLA confidentiality requirements. This indicates a need to understand various SLA confidentiality requirements that exist among the GAs when using such remote services offered by external SPs.

To increase the consideration of confidentiality and security requirements in SLA definition, it is necessary that external SPs should understand government SLA confidentiality requirements, as well as what types of government assets to protect and what types of risks to mitigate. However, the formulation of SLA confidentiality requirements has not been deeply studied by academic computer security community. We seek to fill the gap by understanding government's perspective about SLA confidentiality requirements, which are targeted at participants who are employed by or have experience working with government agencies using Indonesia as a case study.

To this end, we develop a grounded understanding of SLA confidentiality requirements for service provision using a grounded adaptive Delphi study [11]. Following accepted a Delphi study for qualitative study to elicit the views of government participants, we conducted a grounded Delphi study by asking 35 participants via group discussions and individual sessions [11] [12] and conducting a grounded theory analysis [13]–[15] of the Delphi study data to categorise the extracted statements.

Based on our preliminary findings, there are undeveloped government SLA confidentiality requirements, which might arise from the fact that our participants were influenced by existing security standards. However, our study can be used to guide the creation of trustworthy SLA capabilities a means of incorporating confidentiality requirements and capabilities in the formulation of security-related SLAs.

The remainder of this paper is structured as follows: In Section 2, we provide a background of this study. Section 3 presents the research methodology. Section 4 reports key findings. Section 5 discusses the implications of our findings, followed by the limitations of the study. We conclude this paper in Section 6.

II. Background

Some governments have taken steps to reduce the level of cybersecurity risk, especially for government procurement of external computing, communications and storage products and services supplied by SPs or suppliers. We provide context for our study by looking at other governments' security requirements, such as the UK, the US and China.

The UK government has introduced cybersecurity requirements, called 'Cyber Essentials, which is intended for external SPs or suppliers that handle sensitive government data and personal information [16]. There are five technical security controls required for basic security requirements against common types of cyberattacks in such a government organisation. The cybersecurity requirements are *boundary firewalls, Internet gateways, secure configurations, access control mechanisms, malware protection systems, and patch management tools*. As a consequence, these minimum security requirements must be addressed by suppliers or contractors seeking to conduct business with the UK government.

Additionally, the Cyber Essentials is a continuous effort by the UK government to address cybersecurity risk, following the success of the 10 Steps of Cybersecurity guidance, which is designed for organisations as an effective means to protect information assets from cyber threats or attacks [17]. The security requirements are *risk management, secure configuration, network security, managing user privileges, user education and awareness, incident management, malware prevention, monitoring, removable media controls and home and mobile working*. The present requirements are significant for establishing the effectiveness of basic security controls against cyber threats.

Similarly, any potential and existing providers or contractors working with the U.S. Federal agencies are required to meet cybersecurity requirements described in NIST SP800-171 [18]. The standard consists of 14 security requirements, which are adapted from FIPS 200 and NIST SP800-53. Those requirements are *access control*, *awareness and training*, *audit and accountability*, *configuration management*, *identification and authentication*, *incident response*, *maintenance*, *media protection*, *personnel security*, *physical protection*, *risk assessment*, *security assessment*, *system and communication protection* and *system and information integrity* [19]. The derived security requirements are intended for use by federal agencies and for protecting the confidentiality of any information that law, regulation or policy requires to have security controls [18]. However, the NIST standard does not deal with information integrity or availability and aim to clarify specific security requirements applied to SPs or contractor who process or store sensitive government data on their information system services [18].

Furthermore, the NIST SP 800-171 standard is intended for suppliers or contractors that want to use internal cloud-based services as part of its internal enterprise network systems to process, store or transmit data when performing under the government contract requirements (e.g. DoD contract). However, it does not apply when suppliers or contractors intend to use external computing, communications and storage services provided by other external providers to store, process or transmit any sensitive data for the contract. Such suppliers or contractors need to apply security controls and independent assessments from the Federal Risk and Authorisation Management Program (FedRAMP) [20] when acquiring a variety of cloud-based services from other external providers, which are required to comply with security requirements contained within DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012. The security requirements are as follows: cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment [21].

Likewise, the government of China has also proposed cybersecurity requirements for external suppliers that provide hardware and software to the banking industries in China. Those proposed security requirements include *source code disclosure*, *local presence*, *intellectual property rights*, *local encryption technology*, *regulatory backdoor* and *risk assessment* [22]. For example, the government approval is required for all products containing encryption technology of which cryptographic algorithms and encryption keys are required to disclose to the government. It is somewhat surprising that the government does not allow the import of foreign encryption technologies. The regulation does not give detailed guidance on the scope of this national security examination and how it will be implemented [22].

Overall lack of security considerations, especially data confidentiality and integrity in SLAs has remained as an open issue for many years. Research continues about the best approach for incorporating security capabilities into the formulation of security-related SLAs. Many governments to date have tended to focus on the use of certification schemes to evaluate security controls to ensure the controls are effective against identified risks [23]. Whereas, an assurance technique based on SLAs has only been applied to regulate service availability and quality of service (QoS). So far, no research has been found about understanding SLA confidentiality requirements in service provisioning.

III. The Study

This paper investigates government SLA confidentiality requirements by means of 35 participants based in Indonesia using a grounded adaptive Delphi study [11]. We use Indonesia as a case study because according to Article 12 of Indonesian Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012, electronic system operators including SPs have obligations to ensure agreements on minimum service level and information security when providing such external service provision to GAs.

A. Ethical Consideration

Approval to conduct this study was obtained from the central university research ethics committee, University of Oxford. Research consent from participants was obtained after email communications. The participants were told the objective of the study, and asked for their involvement in the study. Our participants were voluntary and anonymous and they had the right to drop out in any round.

B. Recruitment

We recruited our participants for the Delphi study via our existing connections to the government employees including government consultants, usually via verbal or email communications with the participants, followed by an email containing an official invitation letter from the government ministry who looks after information assurance and security in Indonesia. In communication with the participants, we stressed a desire for balance in terms of participants' technical expertise and their involvement in policy-making process to achieve meaningful results and keep the failure rate as low as possible [12].

Before the study began, we gave participants a clear understanding of the problem statements along with the initial research questions to all invited participants before they agreed to participate in our series of data collection activities. Finally, we engaged with 35 of 45 invited participants. Most group discussions and individual sessions were conducted in-person, although some were conducted via Skype.

For this study, we limited our participants to those who were directly employed by or have experience working with Indonesian government. This focus allowed us to explore the problem of preserving the confidentiality of sensitive data across GAs. Our government participants came from a diverse work experience and technical backgrounds, such as cyber defence experts, malware experts, cryptography experts, pentesters, and information security management experts. Also, 12 participants hold a PhD degree in information technology-related topics and most participants hold security certifications. To maintain anonymity, we refer to the participants using labels P1 to P35, respecting the participant's identification. We will provide a summary of the participants, but the information given will be anonymised[1]

C. Delphi Study Procedure

We collected data primarily through a three-round Delphi study with 35 participants. We use some features of Delphi, such as group responses with group discussions for eliciting collective views and individual sessions with semi-structured interviews for collecting individual views where participants may not wish to elaborate in a group discussion. Unlike other Delphi studies [24], [25], this study used focus groups and interviews instead of questionnaires as the instrument for data collection because the questionnaires are impractical for the purpose of eliciting genuine views or thoughts from elite participants, such as senior government officials.

1) Round 1: Kick-Off Meeting: We conducted a kickoff meeting with government employees from the Indonesian Directorate of Information Security who looks after information security and assurance across all government agencies in Indonesia. This round was intended to gather comments and recommendations regarding the Delphi questions and other material. This stage was also important to refine the Delphi questions for the next round of Delphi.

2) Round 2: Brainstorming Phase: The second step was the brainstorming phase with exploratory group discussions with government participants. We conducted a series of group discussions to adapt the work schedules of government participants when participating in group discussions. Each panel discussed the problem of preserving the confidentiality of sensitive data across government agencies. Furthermore, we asked participants to explore Article 12 of the Government Regulation Number 82 of 2012. Also, we asked the participants how to incorporate confidentiality requirements and capabilities specified into SLAs according to reasonable risks.

For this round, we engaged with 18 of the 45 invited participants in three group discussions to explore a rich understanding of participants' experiences and beliefs, as well as to generate information on collective views [26] in which the optimum size for a focus group is 6 to 11 participants [26]. However, in practice, focus groups can work successfully with from three to fourteen participants [27]. For this study, the focus group varies from three participants to six participants to provide control over the period from securing participant work schedules to participating group discussions.

3) Round 3: Enrichment and Generalisation Phase: We conducted individual sessions using semi-structured interviews to elicit detailed information from government participants based on the results of the previous round. We sent the initial results of the first round in the form of Delphi questions and asked again 45 invited participants to take part in this study. In this round, we engaged with 32 government participants and recorded each individual interview in an audio format after receiving the participant's consent. Each individual interview took between 20-120 minutes. Interviews were later transcribed and coded. We then sent each transcription to the corresponding participants and asked for feedback and corrections, which we did not receive any.

D. Data Analysis

We applied the grounded theory analysis [13]–[15] to examine the Delphi study data, and to categorise and generalise the extracted statements. We conducted initial coding of a group discussion transcript from the brainstorming phase to identify general codes. Further, we analysed the interview transcripts from the enrichment and generalisation phase, using initial coding, intermediate coding and advanced coding [28].

The initial coding aims to identify topic of interest 'key-point coding' of which the researcher extracted useful sentences or statements and applied codes against the Delphi study data. In intermediate coding, we began to select categories from amongst topics of interest and found relationships among the initial codes (e.g. the most frequent or important codes) [15]. In advance coding, once categories were identified, we established the relationship between the categories to integrate them into a cohesive theory.

To illustrate the grounded theory process, we provide an example as follows. One participant commented that the greater threat to GAs mostly come from internal sources, such as an insider threat. We coded it as "collaborator", as described in Table II. Our Delphi study data were coded only by the main researcher due to confidentiality reasons. Thus, this was the rationale behind our decision to use the main researcher as the only coder. However, the main researcher discussed his findings with another researcher to receive feedback.

IV. Results

We organise our results into three themes: (1) *government asset*, (2) *risk perception* and (3) *SLA confidentiality requirements*. These findings reveal opportunities for improving the consideration of security requirements in SLA definition.

A. Government Asset

We began by looking from the perspective of what types of government assets to protect by identifying government data. Several statements have been made by participants related

[1] Participants information, https://goo.gl/w0Y4Sz, (Accessed March 2017).

to government assets-based data classification. However, we noticed that the classification of sensitive government data has not been clearly defined. Therefore, we highlight the notion of government assets where applicable, as shown in Table I.

TABLE I. GOVERNMENT ASSET

Category	Government Data
Human Asset	Senior Government Officials Knowledge Others
Information Asset	Citizen Data Medical Record Financial Transaction Law Enforcement Data Diplomatic Information Personal representative deed Personally identifiable information National economic resilience Natural wealth/resources
Physical Asset	National defense and security systems Critical National Infrastructure Communication Servicea and Devices

1) Human Asset: Our participants agreed that human assets (e.g. employees, senior government officials) are part of intangible assets that the government has. Although the Public Information Disclosure Act No 14 of 2008 does exist, our participants typically reported that most GAs face a challenge of classifying sensitive human assets and non-sensitive human assets. Therefore, we placed emphasis on opinions from government participants regarding the concepts of sensitive human assets, such as the following:

> "*...In relation to human assets, if the person is a senior government official who performs such activities, the person itself is a national asset that needs to be protected...*" (P8).

2) Information Asset: Many public organisations routinely collect, create or process sensitive data. Our participants expressed concern in response to protecting information assets data that may not be appropriate for public release. For example, P2 indicated the following:

> "*...In government sectors, it looks "gray", for example, one has uploaded the entire local government meetings including their internal meetings to Youtube, with the aim to build trust to the public. However, all information related to strategic meetings should be protected...*"(P2).

3) Physical Asset: Although it used to be that security objectives were focused in protecting physical assets, such as communication channels, systems and devices, our participants considered the importance of protecting physical assets containing sensitive government data. Securing information assets is critical and may be more than important than protecting physical assets. For example, P1 pointed out the following:

> "*...such electronic information requires physical facilities like data centre, network, systems and devices. It is also necessary to ensure safety and effective physical protection for the facilities...*"(P12).

Our participants indicated that there is an absence of government security classifications that apply to the GAs, which generate, process, collect, store or transmit sensitive data in order to conduct government activities and to deliver public services. In response to this, the government should classify government data so that everyone who works with the GAs knows how best to protect sensitive data.

B. Risk Perception

We carefully examined specific risks that our participants are attempting to counter. Several statements have been made by participants related to risks that need to be mitigated. We noticed consensus was obtained regarding a specific risk and highlight the notions of threat models where applicable, as shown in Table II.

TABLE II. RISK PERCEPTION

Category	Threat/Attack
Collaborator	Insider (Employee) Insider (Former employee) Insider (Contractor) Malicious actions (Service provider)
Exfiltration	Connect-Transmit (Device) Outbound (Traffic) Extract (Content/Key) Brute-force (Key)
Observation	Discovery (State actor) Scan (Metadata/Traffic) Intercept (Device/Content/Traffic)
Insertion	Inject (Malware/Trojan/Backdoor/Scripts) Install (Ransomware/Rootkit)
Manipulation	Manipulate-Phishing (People/Content) Impersonate (People/System/Traffic)

1) Collaborator: Our participants discussed this threat as the main security concern, which allows a person to cooperate traitorously with an adversary. Therefore, our participants paid much attention to mitigating this threat (e.g. insider threats). For example, one participant highlighted that government data leakage is mainly caused by an insider who is a closely related person with senior government officials, as follows:

> "*...the issue about government data theft normally does not occur while data is transmitted, but when data was processed or created. For example, an insider can disclose and share the sensitive data obtained with an adversary...*" (P22).

2) Exfiltration: Our participants were concerned with the unauthorised transfer of sensitive data through various means. For example, one participant indicated the following:

> "*...Now the fact that threats and attacks can actually come from inside. For example, our observation discovered botnets keep sending out data...*" (P13).

3) Observation: Our participants discussed the importance of preventing pervasive surveillance, as this threat allows the adversary to closely observe or monitor targets. One participant indicated this type of threat, as follows:

> "*...we are aware that when we are talking with our interlocutor, there must be other people listening without knowing them...*"(P4).

4) Insertion: Our participants reported that an adversary could place or insert malicious software (malware) on the targeted government's information systems through various methods, as indicated in the following statement:

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

5) Manipulation: Our participants reported that the action of manipulating information systems is an effective way to obtain sensitive data from targets (e.g. people). This allows the adversary to pretend to be another person with the aim of obtaining sensitive government data from the target. For example, P3 pointed out the following statement.

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

Overall, our participants were clear about the perceived shortcomings of the existing knowledge to be used to understand the characteristics of threats. In so doing, it is of paramount importance to enforce SLA confidentiality requirements according to perceived threats for government assets-based data classification in security-related SLAs.

C. SLA Confidentiality Requirements

The statements from our participants confirmed that most government SLA confidentiality requirements are derived from a very high level of abstraction, such as laws, policies, regulations and standards. However, we noticed that the concepts of government SLA confidentiality requirements have not been clearly defined in the context of security-related SLAs. Thus, we highlight the government SLA confidentiality requirements where applicable, as shown in Table III.

1) Skills and Reputation: Our participants reported relatively strong support for inadequate awareness and training for employees, as described the following statement:

> "*...at the simplest level, we still have problems due to lack of awareness of employees, so we need to mitigate such risk...*" (P2).

2) Zero Access to Data: Our participants reported that access control must be in place to ensure that all sensitive government data are limited to authorised users, as follows:

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

3) Personnel Security: Our participants expressed concern about people as a point of security failure, as follows.

> "*...Security screening should be there. Access restriction is based on a need-to-know basis...*" (P6).

TABLE III. SLA CONFIDENTIALITY REQUIREMENTS

Category	**Need**
`Skills and Reputation`	Awareness Training Certification IT Audit and Assurance Penetration Testing
`Zero Access to Data`	Separate duties Control and Limit Connections Privilege Access Control
`Personnel Security`	Implement Screening Identify behaviours Develop Security Culture Non-disclosure agreement (NDA)
`Physical Security`	Physical Access (e.g. Access Card, Keys) Audit logs of physical access CCTV (closed-circuit television) Alarm systsm (sensor)
`Media Protection`	Employ cryptography to protect media Access Control Policy
`Metadata Protection`	Metadata Standard Metadata retention
`Malware Protection`	Employ anti-malware Limit use of external devices
`Communications Protection`	Encryption Secure channels (e.g. VPN Tunnel) Use code in communications
`Data Protection`	Data Localisation IT Audit and Assurance
`Isolation`	Firewall Whitelist Block access to known file transfer Air-gapping
`Authentication`	Multifactor authentication

4) Physical Security: Our participants pointed out that physical security is one of the key security requirements. For example, one participant mentioned physical security measures as described in the following statement:

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

5) Media Protection: Our participants typically reported that it is important to prohibit the use of portable storage devices when such personal devices belong to government employees or contractors, as described in the following statement:

> "*...data storage device should not be brought from outside, everyone who enters, does not allow to bring flash disks, and other media storage...*" (P1).

6) Metadata Protection: Our participants also expressed concerns about metadata protection related to sensitive government data that is processed, stored or transmitted in information system services provided by `SPs`, as follows:

> "*...we should have a metadata standard for the benefit of the government, so that all are used unique, in preventing no data is revealed...*" (P4).

7) Malware Protection: Our participants expressed concern about malware. It is acknowledged that malware can come into our information systems from all types of sources, for instance:

> "*Malware including Ransomware mostly comes from email and web phishing*" (P15).

8) Communications Protection: Our participants reported that network communications are important to be controlled and secure against threats, as follows:

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

9) Data Protection: Our participants expressed concerns about how to protect sensitive government data (the secrecy, integrity and availability of sensitive data). As data resides in many places, one participant expressed in the following case:

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

10) Isolation: Our participants expressed concerns about isolation of communications and information systems to prevent unauthorised disclosure of data, as such the following:

> "*...It is clear that different treatments are required, such as a layer of insulation (e.g., VPN layers). So later, all sensitive data that really matter are protected and isolated using those layers...*" (P8).

11) Authentication: Our participants explicitly mentioned using authentication to access such services, as follows:

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

It is clear that our participants revealed undeveloped government SLA confidentiality requirements. The preference for the requirements was evident even though there would be room for improvement to better define such SLAs.

V. Discussion

We discuss the implications of our findings for `GAs`, `SPs`, and researchers. We consider the following take-aways to be the most important one from our findings.

A. Implications

1) Implications for Government Agencies: Based on our findings, we give two recommendations to `GAs`. First, know your assets. Our study suggests that different assets have different risks associated with it. The `SPs` seem to neglect to consider appropriate security controls for protecting the value of government assets, while the `GAs` do not provide high-level security requirements up-front. In either case, `GAs` should understand what types of confidentiality requirements that need to be defined in SLAs according to acceptable risks that might affect government asset value. Second, understanding the risks to government assets. We found that specific threats are typically scattered across different participants. However, some conclusions were drawn from the findings concerning risk perception. Thus, `GAs` should identify which perceived threats are mitigated best by security capabilities (e.g. security controls) provided by external `SPs`.

2) Implications for Service Providers: It is acknowledged that many `GAs` commonly make decisions to preserve the confidentiality of government data by applying specific security capabilities through technical, physical and human elements. In this case, the `GAs` heavily rely on certification schemes such as ISO 27001, which is not sufficient to address specific perceived and emerging threats [23]. Our study shows that the derived findings provide basic insights into defining confidentiality requirements in SLAs. Thus, the `SPs` can determine and negotiate appropriate security capabilities, which demonstrate compliance with the government's security requirements. In the context of formulation of security-related SLAs, the level of trust between the `GAs` and external `SPs` can be determined by using confidentiality capabilities according to specific perceived threats for government assets-based data classification.

3) Implications for Researchers: Finally, our findings can provide a rich foundation for incorporating the interplay of perceived threats, security requirements and capabilities specified in SLAs according to government assets. However, we acknowledge that it is difficult to require explicit assumptions about confidentiality requirements and capabilities regarding perceived threats for government assets. Often, there is the risk of liability and compensation with the particular level of security expressed in SLAs. These questions sketch many avenues for future work.

B. Limitations

As with any research methodology, our choice of research methods has limitations.

1) Construct Validity: It is important to measure whether these findings can be correctly reflected by means of Delphi study. First, group discussions and individual feedback obviously rely on the statements of the participants. Insights and views from the participants are subjective and may not properly reflect the actual situations. However, we engaged with experienced participants from different expertise to gain a broader spectrum of viewpoints. While subjectivity is difficult to eliminate in a qualitative study, we limit its effects by basing our findings exclusively on multiple statements from a series of iterative data collection activities using group discussions and individual sessions. Further, the nature of our Delphi study allowed us to react to participants' statements, and to further clarify, whenever needed. Second, there are possible misperceptions associated with the interpretation of the statements by the main researcher. The coding process was performed manually and by only one researcher, which potentially a biased to the interpretation of the data. To mitigate this threat, we asked feedback from the participants.

2) Internal Validity: Since our study is of exploratory nature, our preliminary findings are determined mainly by the Delphi study data we have obtained from 35 selected government participants through a purposeful sampling strategy. We selected participants across Indonesian government employees including participants with a wide variety of insights and opinions as it is expected from the nature of Delphi study. This study is completely recorded that provides full traceability of findings back to the original statements from our participants.

3) External Validity: The applicability of our findings has to be established carefully. The main limit to the generalizability of our findings from the fact that we only engaged with 35 participants from one country. Although our findings may be applicable only to the domain and context being studied [15], the results of this study can illuminate other governments to include security capabilities of the service providers in SLAs when procuring such external computing, communications and storage services. We could increase confidence by involving more government participants in the country or from other countries may create a more rigorous findings. Bearing in mind that this study is of exploratory of nature and was not designed to be largely generalizable, but it aimed to understand what are the SLA confidentiality requirements needed from the government.

VI. Conclusion

It is acknowledged that, until now, security best practices and standards are often considered to be key elements of implementing and enforcing the most basic security requirements. However, government SLA confidentiality requirements have not been studied in depth by governments, providers, and researchers. To address this gap and inform ongoing and future work on external computing, communications and storage service provision, we conducted a grounded adaptive Delphi method with 35 government participants using Indonesia as a case study. Most importantly, we found that government SLA confidentiality requirements have seen limited demand for services provision in government contracts relating to external computing, communications and storage services supplied by external SPs. However, our findings provide insights to increase the consideration of confidentiality and security requirements in SLA definition. These findings suggest that there is a need for an approach to incorporate security capabilities specified in security-related SLAs to enhance the level of trust in service provision, such as cloud-based services between GAs and external SPs. We take an important step towards such an empirically grounded trustworthy SLA capabilities for incorporating security requirements and capabilities into security-related SLAs according to perceived risks for government assets-based data classification.

VII. Acknowledgment

This work was supported in part by the Indonesian Ministry of Communications and Information Technology under the Directorate of Information Security, and the Indonesia Endowment Fund for Education Scholarship (LPDP).

References

[1] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, and U. Villano, "Security as a service using an sla-based approach via specs," in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science, vol. 2, 2013, pp. 1–6.

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

[3] "SLAReady," 2015, URL: http://www.sla-ready.eu/consortium [accessed: 2017-07-15].

[4] "SLALOM Project," 2015, URL: http://slalom-project.eu/ [accessed: 2017-07-15].

[5] R. R. Henning, "Security service level agreements: Quantifiable security for the enterprise?" in Proceedings of the 1999 Workshop on New Security Paradigms (NSPW), 2000, pp. 54–60.

[6] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security slas for federated cloud services," in 6th International Conference on Availability, Reliability and Security, Aug 2011, pp. 202–209.

[7] M. G. Jaatun, K. Bernsmed, and A. Undheim, Security SLAs – An Idea Whose Time Has Come? Springer, 2012, pp. 123–130.

[8] A. Guesmi and P. Clemente, "Access control and security properties requirements specification for clouds' seclas," in 5th IEEE International Conference on Cloud Computing Technology and Science, vol. 1, Dec 2013, pp. 723–729.

[9] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative reasoning about cloud security using service level agreements," IEEE Transactions on Cloud Computing, vol. PP, no. 99, 2017, pp. 1–1.

[10] T. Takahashi, J. Kannisto, J. Harju, S. Heikkinen, B. Silverajan, M. Helenius, and S. Matsuo, "Tailored security: Building nonrepudiable security service-level agreements," IEEE Vehicular Technology Magazine, vol. 8, no. 3, Sept 2013, pp. 54–62.

[11] Y. Nugraha and A. Martin, Investigating Security Capabilities in Service Level Agreements as Trust-Enhancing Instruments. Cham: Springer International Publishing, 2017, pp. 57–75.

[12] Y. Nugraha, I. Brown, and A. S. Sastrosubroto, "An adaptive wideband delphi method to study state cyber-defence requirements," IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 1, 2016, pp. 47–59.

[13] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner, "Investigating the computer security practices and needs of journalists," in 24th USENIX Security Symposium, Washington, D.C., 2015, pp. 399–414.

[14] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in 21st ACM Conference on Computer and Communications Security, 2014, pp. 750–761.

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

[16] "Procurement policy note-use of cyber essentials scheme certification," 2016, URL: https://www.gov.uk/government/collections/procurement-policy-notes [accessed: 2017-07-15].

[17] "National Cyber Security Centre: 10 Steps to Cyber Security," 2016, URL: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security [accessed: 2017-07-15].

[18] "DoD Amends its DFARS Safeguarding and Cyber Incident Reporting Requirements with a Second Interim Rule," 2016, URL: http://www.hlregulation.com/2016/01/07/dod-amends-its-dfars-safeguarding-and-cyber-incident-reporting-requirements-with-a-second-interim-rule/ [accessed: 2017-07-15].

[19] R. Ross, P. VISCUSO, G. GUISSANIE, K. DEMPSEY, and M. RIDDLE, "Protecting controlled unclassified information in nonfederal information systems and organizations," NIST Special Publication, vol. 800, 2015, p. 171.

[20] "Federal risk and authorization management program," 2016, URL: https://www.fedramp.gov/resources/documents-2016/ [accessed: 2017-07-15].

[21] E. P. Roberson, "Adequate cybersecurity: Flexibility and balance for a proposed standard of care and liability for government contractors," Fed. Cir. BJ, vol. 25, 2015, p. 641.

[22] "China introduces new cybersecurity for rules for banking procurement," 2015, URL: http://knowledge.freshfields.com [accessed: 2017-07-15].

[23] R. Böhme, Security Audits Revisited. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 129–147.

[24] T. Päivärinta, S. Pekkola, and C. E. Moe, "Grounding theory from delphi studies," in International Conference on Information Systems, vol. 3. Association for Information Systems, 2011, pp. 2022–2035.

[25] K. Howard, "Educating cultural heritage information professionals for australia's galleries, libraries, archives and museums: A grounded delphi study," Ph.D. dissertation, Queensland University of Technology, 2015.

[26] M. C. Harrell and M. A. Bradley, "Data collection methods. semi-structured interviews and focus groups," RAND National Defense Research Institute Santa Monica-CA, Tech. Rep., 2009.

[27] P. Gill, K. Stewart, E. Treasure, and B. Chadwick, "Methods of data collection in qualitative research: interviews and focus groups," British dental journal, vol. 204, no. 6, 2008, pp. 291–295.

[28] M. Birks and J. Mills, Grounded theory: A practical guide. Sage, 2015.