MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

First edition
2020-05-05

Guidelines for Securing Cloud Implementation by Cloud Service Subscriber

Reference number:
MySEF-5-GUI-15-CLOUDSEC_GUI_CSS-v1

REGISTERED OFFICE:

CyberSecurity Malaysia,
Level 7 Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia
Email: mysef_bd@cybersecurity.my

DISCLAIMER

This document is for informational purposes only. It represents the current thinking of CyberSecurity Malaysia on the security aspects of the Cloud Computing environment. It does not establish any rights for any person and is not binding on CyberSecurity Malaysia or the public. The information appearing on this guideline is not intended to provide technical advice to any individual or entity. We urge you to consult with your organization before taking any action based on information appearing on this guideline or any other documents to which it may be linked.

Table of Contents

1 Introduction

1.1 Overview

Cloud computing services provide a fast, convenient, cost-saving and minimal workflow environment. Thus, most companies set up their workspace on the cloud environment for easy access via the Internet.

In providing cloud computing services, Cloud Service Provider (the Provider) offers three types of cloud service models which are the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) models. As for Cloud Service Subscribers (the Subscriber), cloud computing services allow them to have flexible IT solutions to be deployed without the needs to procure physical IT infrastructures such as servers, storage, and processing components. Thus, adequate security controls to ensure the confidentiality, integrity and availability are required in protecting Cloud Service Subscriber data.

This document is prepared for Subscriber to understand public cloud subscription that focuses on IT security perspective covering three (3) stages: 1) pre-subscription, 2) during subscription and 3) post-subscription of IaaS, PaaS and SaaS models.

This document also serves as the guidelines for Subscribers to understand cloud security features that should be applied to the different cloud service models at different subscription stages.

1.2 Scope

This document focuses on public cloud security guidance for Subscribers.

This document covers security requirements to be implemented by Subscribers in subscribing to services offered by three types of cloud service models: IaaS, PaaS and SaaS.

1.3 Objective

The objectives of this guideline are as follows:

a) To provide cloud security guidance to Subscribers on public cloud services.

b) To provide a mapping of security controls based on the subscription stages of cloud services to the relevant cloud standards.

1.4 Intended Audience

The intended audience for this document is the Subscribers that refers to the following crowds, as stated below:

a) Public Sectors; and

b) Private Sectors (e.g. individual for personal usage, the organization for business and operational use managed by relevant person-in-charge such as IT Technician, Chief Information Security Officer (CISO) and IT Administrator).

1.5 Rationale

The guideline is prepared based on the following rationales:

a) To support the current cloud computing technology initiatives, challenges and demands (request) from the local IT industry.

b) To support and provide a basis of understanding on cloud computing requirements that is applicable for IR4.0 based on the Industry4WRD: National Policy for Industry 4.0 [1] under the Cyber Security, Cloud Computing and IoT pillars.

c) It is a publicly accessible document that describes the cloud security controls based on the cloud subscription stages (pre-subscription, during subscription and post-subscription). A mapping of the cloud security controls, with the respective standards, for each stage of cloud service subscription is presented in section 4. The mapping aims to provide a quick guide to the Subscriber in identifying the required/recommended security controls based on ISO/IEC 27036-4:2016(E), Table A.1 (Cross-references for cloud services and deployment models and relevant standards) at the different stages of the subscription. The cloud extended security controls that are not covered in ISO/IEC 27036-4:2016(E) is defined in Bibliography.

2 Terms, Definitions and Abbreviated Terms

2.1 Terms and Definitions

For the purpose of this document, the following terms and definitions applied.

2.1.1 Cloud Service Provider

The Cloud Service Provider is an organization and the entity responsible for making a service available to interested parties.

Note 1: A Cloud Service Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Subscriber through network access.

Note 2: Also refer as the Provider.

2.1.2 Cloud Service Subscriber

The Cloud Service Subscriber is the principal stakeholder for the cloud computing service.

Note 1: A Cloud Service Subscriber represents a person or organization that maintains a business relationship with and uses the service from a Cloud Service Provider.

Note 2: Also refer as the Subscriber.

2.1.3 Organization

The organization who subscribes, purchases or leases the cloud services and solutions from the Cloud Service Provider. E.g. government agencies small medium enterprise or financial institution.

2.2 Abbreviated terms

For the purposes of this document, the following abbreviations apply.

AES	Advanced Encryption Standard
API	Application Programming Interface
CISO	Chief Information Security Officer
CSM	CyberSecurity Malaysia
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
ID	Identity Document
IT	Information Technology
NTP	Network Time Protocol
OS	Operating System
PaaS	Platform as a Service
RSA	Rivest-Shamir-Adleman Encryption Algorithm
SaaS	Software as a Service
SHA	Secure Hash Algorithms
SLA	Service Level Agreement
TAC	Transaction Authorisation Code
TLS	Transport Layer Security
VAPT	Vulnerability Assessment and Penetration Testing
VM	Virtual Machine

3 Overview of Cloud Computing

This section provides an overview of the cloud computing service models and deployment models. A comparison of the deployment models is presented to give a clearer picture of the differences between these models.

3.1 Cloud Computing Service Model

There are three (3) types of cloud computing service models in the cloud computing operational environment, which are SaaS, PaaS, and IaaS, as shown in Figure 1.

Figure 1: Cloud Computing Service Models

The definitions for each type of cloud computing services[1] by ISO/IEC 17788:2014(E) are as follows:

a) **Software as a Service (SaaS)** - A cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

b) **Platform as a Service (PaaS)** - A cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

c) **Infrastructure as a Service (IaaS)** - A cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

[1] Based on ISO/IEC 17788:2014(E), Section 6.4, Cloud capabilities types and cloud service categories.

3.2 Cloud deployment models

The cloud computing deployment models are divided into four (4) types by ISO/IEC 17788:2014(E) as follows:

a) **Public Cloud** is a deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider. A public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud service provider. Actual availability for specific cloud service customers may be subject to jurisdictional regulations. Public clouds have very broad boundaries, where cloud service customer access to public cloud services has few, if any, restrictions.

b) **Private Cloud** is a deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer. A private cloud may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. The cloud service customer may also authorise access to other parties for its benefit. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization.

c) **Hybrid Cloud** is a deployment model using at least two different cloud deployment models. The deployments involved remain unique entities but are bound together by appropriate technologies that enable interoperability, data portability and application portability. A hybrid cloud may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. Hybrid clouds represent situations where interactions between two different deployments may be needed but remained linked via appropriate technologies. As such the boundaries set by a hybrid cloud reflect its two base deployments.

d) **Community Cloud** is a deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this community. A community cloud may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. Community clouds limit participation to a group of cloud service customers who have a shared set of concerns, in contrast to the openness of public clouds, while community clouds have broader participation than private clouds. These shared concerns include, but are not limited to, mission, information security requirements, policy, and compliance considerations.

The cloud computing deployment models are divided into four (4) types by ISO/IEC 17788:2014(E) as follows:

Table 1: Comparison of Cloud Computing Deployment Models

Model vs Characteristic	Private Cloud	Public Cloud	Hybrid Cloud	Community Cloud
Account Type	Single Tenant	Multi-tenant	Combination, Private or Public cloud.	A multi-tenant platform that is accessible only for a specific subset of customer
Premises Type	Owned premises and managed by the organization	Owned and managed by the service Provider. Off-premises / Third Party	Owned and managed by multiple organization	Owned and managed by multiple organization
Data Management Type	Data management policy is self-managed by the organization.	Data management policy is bound to the multi-tenant data policy.	Each organization manages data management policy.	Data management policy should be managed by an organization.
Security Management	Dependent on own organization security management	Dependent on own organization security management by the Provider and the Subscriber	Dependent on own organization security management by the Provider and the Subscriber	Dependent on own organizations' security management in the community
Data Classification	The Subscriber should identify risks based on data classification that will be hosted on the cloud (e.g. Top Secret, Secret, Confidential, Restricted and Public). For Subscribers from the public sectors, they may refer to Malaysian Government Policies such as "Official Secrets Act (OSA)".			

3.3 Cloud Security Controls

The critical security controls of cloud computing service models are elaborated as follows;

a) Basic operations of each cloud computing service model and type of services being offered to the Subscriber;
b) The list of security controls and its elaboration in this document will help the Subscriber as a guideline;
c) Roles and responsibilities of the Subscriber in ensuring security features and functions are being implemented accordingly by the provider; and
d) Crucial information and essential aspects that the Subscriber should be aware of when subscribing to cloud service models from the provider such as Service Legal Agreement (SLA), the scope of services, termination clauses, and action items to ensure continuous IT security implementation.

The details of typical threats and risks with their associated security controls are further explained in Section 4.

3.4 Risk Assessment

It is recommended for the Subscriber to perform risk assessment to understand security risks that may exist and implement security controls in mitigating them . If the controls are not applicable to the Subscriber, it is recommended for the Provider to comply with minimum security controls defined in the ISO/IEC 27017:2015(E) and ISO/IEC 27002:2013(E).

In the event of the Subscriber require to perform risk assessment, the Subscriber may refer to the template of risk assessment based on the link provided below.

http://download.microsoft.com/documents/australia/enterprise/Risk_Framework_Template_Tool.xlsm

3.5 Selection Criteria of the Cloud Service Provider

It is recommended to select the Provider based on the following criteria;

The Provider should comply with the following standards and implement best practices as stated below:

a) ISO/IEC 27001:2013(E) Information technology, Security techniques, Information security management systems, Requirements;
b) ISO/IEC 27017:2015(E) Information technology, Security techniques, Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
c) ISO/IEC 27018:2018(E) Information technology, Security techniques, Code of practice of personally identifiable information (PII) in public clouds acting as PII processors;
d) Payment Card Industry Data Security Standard (PCIDSS);
e) Cloud Security Alliance Cloud Controls Matrix (CSA CCM);
f) Service Organization Control (SOC2); and
g) Personal Data Protection Act 2010 (PDPA).

For the Providers that are certified with ISO/IEC 27001:2013(E) Information Security Management System, the Subscriber should request the Statement of Applicability (SOA) from them to confirm the scope of certification inclusive of their cloud services.

The Subscriber may also refer to Technical Code for Cloud Service Provider Selection document by Malaysian Communications & Multimedia Commission (MCMC) and Malaysian Technical Standards

Forum Bhd (MTSFB) for the provider selection, entitled Information and Network Security – Cloud Service Provider Selection (MCMC MTSFB TC G017:2018).

3.6 The Subscriber and the Provider Responsibilities

Figure 2 illustrates the responsibilities of the Provider and the Subscriber in the cloud service models offered by the Provider.

	INFRASTRUCTURE AS A SERVICE (IAAS)	PLATFORM AS A SERVICE (PAAS)	SOFTWARE AS A SERVICE (SAAS)
USER	SUBSCRIBER	SUBSCRIBER	SUBSCRIBER
DATA	SUBSCRIBER	SUBSCRIBER	SUBSCRIBER
APPLICATIONS	SUBSCRIBER	SUBSCRIBER	PROVIDER
OPERATING SYSTEM	SUBSCRIBER	PROVIDER	PROVIDER
VIRTUAL NETWORKS	SUBSCRIBER	PROVIDER	PROVIDER
HYPERVISORS	PROVIDER	PROVIDER	PROVIDER
SERVERS AND STORAGE	PROVIDER	PROVIDER	PROVIDER
PHYSICAL NETWORKS	PROVIDER	PROVIDER	PROVIDER

Figure 2: The Provider and the Subscriber Responsibilities in Cloud Service Model

When choosing a cloud service model (IaaS, PaaS, or SaaS), the Subscriber should consider which of the service model can accommodate the requirements set by the individual or organization business operations. This includes the different type of security requirements made available by the Provider for each cloud service models.

Examples of other cloud service models are outsourcing models such as Test as a Service, Security as a Service, Mobile as a Service etc.

3.7 Cloud Deployment Models

The cloud deployment models offered by the Provider are illustrated in Figure 3.

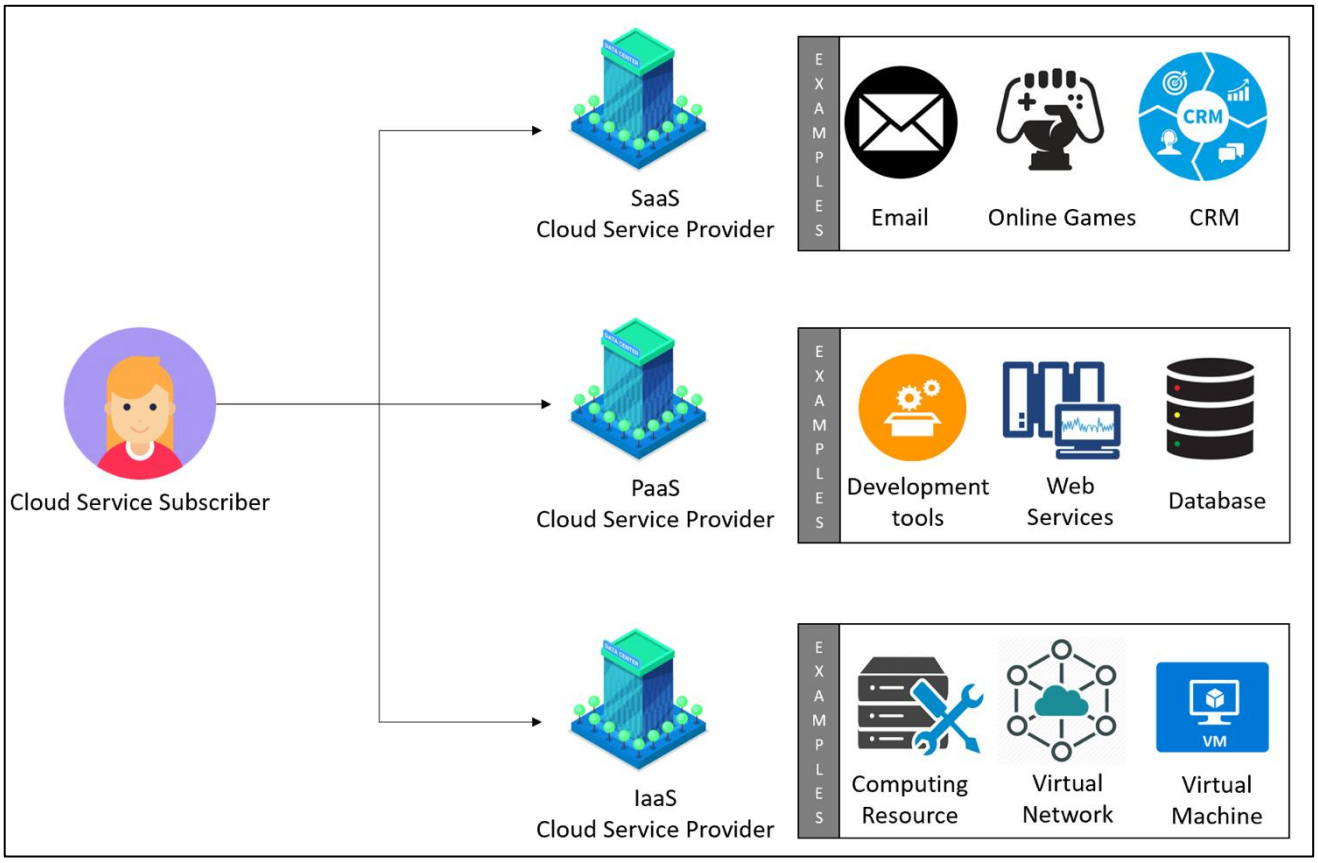

Figure 3: Cloud Deployment Models

Examples of Software as a Service (SaaS) such as Microsoft Office 365, Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur and GoToMeeting.

Examples of Platform as a Service (PaaS) such as AWS Elastic Beanstalk, Microsoft Azure, Heroku, Force.com, Google App Engine and OpenShift.

Examples of Infrastructure as a Service (IaaS) such as DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure and Google Compute Engine (GCE).

4 Threats and Risks in the Cloud Service Model based on Subscription Stages

This section provides the list of 13 common threats and risks of the cloud service model based on reference in the ISO/IEC 27036-4:2016(E) (Refer to Table 2).

Risks and threats for each stage of the cloud subscription; Pre, During and Post as shown in Table 2 are associated with risks and threats as discussed in Table 1 of ISO/IEC 27036-4:2016(E). Controls for each subscription stage for every cloud service model are referred to relevant controls discussed in ISO/IEC 27017:2015(E) and ISO/IEC 27002:2013(E).

If the controls are not applicable to the Subscriber , it is recommended for the Provider to comply with minimum security controls defined in the ISO/IEC 27017:2015(E) and ISO/IEC 27002:2013(E). Otherwise, the Subscriber should perform proper risk assessment to understand the risk that might be present.

Table 2: Threats and Risk mapped to Cloud Service Models based on Subscription Stages

No	Typical threats and risks (based on ISO/IEC 27036)	Subscription Stage	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
1	Lack of control on where the the subscriber data are stored	PRE	Where the Subscriber data are stored **<Control: 13.10>**	Where the Subscriber data are stored **<Control: 10.5>**	Not applicable to the Subscriber
		DURING	Where the Subscriber data are stored **<Control: 14.10>**	Where the Subscriber data are stored **<Control: 11.5>**	
		POST	Not applicable to the Subscriber	Not applicable to the Subscriber	
2	Unknown access to stored the subscriber data	PRE	Who has access to the stored the Subscriber data **<Control: 13.11>**	Who has access to or availability of stored the Subscriber data **<Control: 10.1>**	Who has access to or availability of stored the Subscriber data **<Control: 7.6>**
		DURING	Who has access to or availability of stored the Subscriber data **<Control: 14.11>**	Who has access to or availability of stored the Subscriber data **<Control: 11.1>**	Who has access to or availability of stored the Subscriber data **<Control: 8.6>**
		POST	Not applicable to the Subscriber		
3	Unknown data transmission process	PRE	How the Subscriber data are communicated **<Control: 13.2>**	How the Subscriber data are communicated **<Control: 10.6>**	How the Subscriber data are communicated **<Control: 7.7>**

No	Typical threats and risks (based on ISO/IEC 27036)	Subscription Stage	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
		DURING	How the Subscriber data are communicated **<Control: 14.2>**	How the Subscriber data are communicated **<Control: 11.6>**	How the Subscriber data are communicated **<Control: 8.7>**
		POST	Not applicable to the Subscriber		
4	Unknown superuser, administrator or privileged user access	PRE	Not applicable to the Subscriber Note: May relevant that have unknown superuser account (that is not known by the Subscriber).		
		DURING			
		POST			
5	Lack of protection against malware	PRE	How clearly malware protection is defined **<Control: 13.4.1>**	How clearly malware protection is defined related to insecure platforms **<Control: 10.7>**	How clearly malware protection is defined related to applications **<Control: 7.8>**
		DURING	How the Subscriber manage and monitor malware protection **<Control: 14.4.1>**	How the Subscriber manage and monitor malware protection provided by the Provider **<Control: 11.7>**	How the Subscriber manage and monitor malware protection provided by the Provider **<Control: 8.8>**
		POST	Not applicable to the Subscriber		
6	Unknown access rights to the subscriber data	PRE	Not applicable to the Subscriber	Is the access and rights, through administrator rights clearly defined in the contract **<Control:10.8>**	Is the access and rights through user rights clearly defined in the contract **<Control:7.9>**
		DURING		How the Subscriber manage access and rights, through administrator rights **<Control:11.8>**	How the Subscriber manage access and rights through user rights **<Control:8.9>**
		POST		Not applicable to the Subscriber	Not applicable to the Subscriber

No	Typical threats and risks (based on ISO/IEC 27036)	Subscription Stage	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
7	Lack of log data	PRE	Not applicable to the Subscriber	Is a log of data clearly defined (traceability and integrity) **<Control:10.9>**	Is the log of data from the application is clearly defined (traceability and integrity) **<Control:7.10>**
		DURING		How the Subscriber can request log of data from the Provider **<Control:11.9>**	How the Subscriber can request log of data from the Provider **<Control:8.10>**
		POST		Not applicable to the Subscriber	Not applicable to the Subscriber
8	Unknown integrity of platforms	PRE	Not applicable to the Subscriber	How integrity of platforms is defined (Example: SQL is not tampered by the third party) **<Control:10.10>**	Not applicable to the Subscriber
		DURING		How integrity of platforms is carried out by the Subscriber **<Control:11.10>**	
		POST		Not applicable to the Subscriber	
9	Uncontrolled application layer changes	PRE	Not applicable to the Subscriber		Are application layer changes defined in the online contract (integrity) **<Control:7.11>**
		DURING			How the Provider notify the Subscriber if application layer changes are made (integrity) **<Control:8.11>**
		POST			Not applicable to the Subscriber

No	Typical threats and risks (based on ISO/IEC 27036)	Subscription Stage	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
10	Lack of security requirement in application layer development	PRE	Not applicable to the Subscriber		
		DURING			
		POST			
11	Inability to retrieve the subscriber data during service provision	PRE	Not applicable to the Subscriber		Service availability offered by the Provider is clearly defined in the SLA **<Control:7.12>**
		DURING			Lack of service or other issues, stopping retrieval of cloud service availability, refer to the SLA **<Control:8.12>**
		POST			Not applicable to the Subscriber
12	Uncertainty about control over the subscriber data during and after service provision	PRE	Poor understanding of ownership of the Subscriber data **<Control:13.12>**	Poor understanding of ownership of the Subscriber data **<Control:10.11>**	Poor understanding of ownership of the Subscriber data **<Control:7.13>**
		DURING	Poor monitoring of the the Subscriber data ownership **<Control:14.12>**	Poor monitoring of the the Subscriber data ownership **<Control:11.11>**	Poor monitoring of the the Subscriber data ownership **<Control:8.13>**
		POST	Improper data migration process during termination **<Control:15.4>**	Improper data transferring process during termination **<Control:12.3>**	Lack of awareness of transferring data during termination **<Control:9.3>**
13	Inability to determine whether the subscriber data have been completely deleted at service termination/ end	PRE	Lack of assurance of the Subscriber data have been deleted **<Control:13.12>**	Lack of assurance of the Subscriber data have been deleted **<Control:10.11>**	Lack of assurance of the Subscriber data have been deleted **<Control:7.13>**
		DURING	Not applicable to the Subscriber		
		POST	Lack of verification for the deleted data **<Control:15.4>**	Lack of verification for the deleted data **<Control:12.3>**	Poor understanding of data wipe process provides by the Provider **<Control:9.3>**

5 Mapping of Cloud Security Controls from ISO/IEC 27036-4 with ISO/IEC 27017 for the Subscriber

This section provides guidance on specific controls associated with each subscription stages (Pre, During and Post), which are based on controls that are defined in ISO/IEC 27036-4:2016(E) (refer to Table 3).

If the controls are not applicable to the Subscriber, it is recommended for the Provider to comply with minimum security controls defined in the ISO/IEC 27017:2015(E) and ISO/IEC 27002:2013(E). Otherwise, the Subscriber should perform proper risk assessment to understand the risk that might be present.

Table 3: Mapping of Cloud Security Controls for the Subscriber

No.	Cloud capabilities type based on ISO/IEC 27036-4	Controls based on ISO/IEC 27036-4	Subscription Stage			Cloud-specific information or controls in ISO/IEC 27017
			PRE	DURING	POST	CLAUSES
1	Infrastructure	a) Controls for network security (including network access)	Management of privileged access rights for IaaS pre-subscription **<Control: 13.1.1>** Segregation in Network for IaaS pre-subscription **<Control: 13.1.2>**	Management of privileged access rights during IaaS subscription **<Control: 14.1.1>** Segregation in Network during IaaS subscription **<Control: 14.1.2>**	Not applicable to the Subscriber	9.2.3, 13.1.3
2	Infrastructure	b) Controls for communication security (including cryptography)	Policy on the use of cryptographic controls for IaaS pre-subscription **<Control: 13.2.1>** Regulation of cryptographic controls for IaaS pre-subscription **<Control: 13.2.2>**	Policy on the use of cryptographic controls during IaaS subscription **<Control: 14.2.1>** Regulation of cryptographic controls during IaaS subscription **<Control: 14.2.2>**	Not applicable to the Subscriber	10.1.1, 18.1.5
3	Infrastructure	c) Controls for storage security (including physical storage and security during the lifecycle)	Inventory of assets for IaaS pre-subscription **<Control: 13.3.1>** Labelling of information for IaaS pre-subscription	Inventory of assets during IaaS subscription **<Control: 14.3.1>** Labelling of information during IaaS subscription	Inventory of assets for IaaS post-subscription **<Control: 15.1.1>** Labelling of information for	8.1.1, 8.2.2, CLD.8.1.5

No.	Cloud capabilities type based on ISO/IEC 27036-4	Controls based on ISO/IEC 27036-4	Subscription Stage			Cloud-specific information or controls in ISO/IEC 27017
			PRE	DURING	POST	CLAUSES
			<Control: 13.3.2> Removal of the Subscriber assets for IaaS pre-subscription **<Control: 13.3.3>**	**<Control: 14.3.2>** Removal of the Subscriber assets during IaaS subscription **<Control: 14.3.3>**	IaaS post-subscription **<Control: 15.1.2>** Removal of the Subscriber assets for IaaS post-subscription **<Control: 15.1.3>**	
4	Infrastructure	d) Malware protection	Controls against malware for IaaS pre-subscription **<Control: 13.4.1>**	Controls against malware during IaaS subscription **<Control: 14.4.1>**	Not applicable to the Subscriber	None
5	Infrastructure	e) Monitoring	Clock synchronisation for IaaS pre-subscription **<Control: 13.5.1>**	Clock synchronisation during IaaS subscription **<Control: 14.5.1>**	Not applicable to the Subscriber	12.4.4
6	Infrastructure	f) Capacity management	Capacity management for IaaS pre-subscription **<Control: 13.6>**	Capacity management during IaaS subscription **<Control: 14.6>**	Not applicable to the Subscriber	12.1.3
7	Infrastructure	g) Identity management	This control covers the privacy on the public cloud - Please refer to ISO/IEC 27018:2014(E) for more details: Clauses: A.1.1, A.2.1, A.4.1, A.5.1, A.5.2, A.9.1			None
8	Infrastructure	h) Incident management	Incident responsibilities and procedures for IaaS pre-subscription **<Control: 13.8.1>** Collection of	Incident responsibilities and procedures during IaaS subscription **<Control: 14.8.1>** Collection of	Not applicable to the Subscriber	16.1.1, 16.1.7

No.	Cloud capabilities type based on ISO/IEC 27036-4	Controls based on ISO/IEC 27036-4	Subscription Stage			Cloud-specific information or controls in ISO/IEC 27017
			PRE	DURING	POST	CLAUSES
			evidence for IaaS pre-subscription **<Control: 13.8.2>**	evidence during IaaS subscription **<Control: 14.8.2>**		
9	Infrastructure	i) Establishment of treatment of intellectual property rights of cloud service customers in case backup services are provided	Intellectual property rights for IaaS pre-subscription **<Control: 13.9.1>**	Intellectual property rights during IaaS subscription **<Control: 14.9.1>**	Intellectual property rights for IaaS post-subscription **<Control: 15.3.1>**	18.1.2
10	Platform	a) Access controls (user and administrative access for both cloud service customer and cloud service Provider)	User registration and deregistration for PaaS pre-subscription **<Control: 10.1.1>** User access provisioning for PaaS pre-subscription **<Control: 10.1.2>** Management of privileged access rights for PaaS pre-subscription **<Control: 10.1.3>** Management of secret authentication information of users for PaaS pre-subscription **<Control: 10.1.4>**	User registration and deregistration during PaaS subscription **<Control: 11.1.1>** User access provisioning during PaaS subscription **<Control: 11.1.2>** Management of privileged access rights during PaaS subscription **<Control: 11.1.3>** Management of secret authentication information of users during PaaS subscription **<Control: 11.1.4>**	User registration and deregistration for PaaS post-subscription **<Control: 12.1.1>** User access provisioning for PaaS post-subscription **<Control: 12.1.2>** Management of privileged access rights for PaaS post-subscription **<Control: 12.1.3>** Management of secret authentication information of users for PaaS post-subscription	9.2.1, 9.2.2, 9.2.3, 9.2.4

No.	Cloud capabilities type based on ISO/IEC 27036-4	Controls based on ISO/IEC 27036-4	Subscription Stage			Cloud-specific information or controls in ISO/IEC 27017
			PRE	DURING	POST	CLAUSES
					<Control: 12.1.4>	
11	Platform	b) Management of logging	Event logging for PaaS pre-subscription **<Control: 10.2.1>**	Event logging during PaaS subscription **<Control: 11.2.1>**	Not applicable to the Subscriber	12.4.1
12	Platform	c) Controls over OS integrity	This is not applicable for Cloud environment due to the Subscriber is not permitted to updates and security patching to existing OS			None
13	Platform	d) Controls over OS change	Change Management for PaaS pre-subscription **<Control: 10.3.1>**	Change Management during PaaS subscription **<Control: 11.3.1>**	Not applicable to the Subscriber	12.1.2
14	Platform	e) Establishment of treatment of intellectual property rights of cloud service customers in case backup services are provided	Intellectual property rights for PaaS pre-subscription **<Control: 10.4.1>**	Intellectual property rights during PaaS subscription **<Control: 11.4.1>**	Intellectual property rights for PaaS post-subscription **<Control: 12.2.1>**	18.1.2
15	Application	a) Controls for access and user rights	Information access restriction for SaaS pre-subscription **<Control: 7.1.1>** Use of privilege utility programs for SaaS pre-subscription **<Control: 7.1.2>**	Information access restriction during SaaS subscription **<Control: 8.1.1>** Use of privilege utility programs during SaaS subscription **<Control: 8.1.2>**	Information access restriction for SaaS post-subscription **<Control: 9.1.1>**	9.4.1, 9.4.4
16	Application	b) Controls for application changes	Change Management for SaaS pre-subscription **<Control: 7.2.1>**	Change Management during SaaS subscription **<Control: 8.2.1>**	Not applicable to the Subscriber	12.1.2
17	Application	c) Controls for application	Securing application	Securing application	Not applicable to the Subscriber	14.1.2, 14.1.3

No.	Cloud capabilities type based on ISO/IEC 27036-4	Controls based on ISO/IEC 27036-4	Subscription Stage			Cloud-specific information or controls in ISO/IEC 27017
			PRE	DURING	POST	CLAUSES
		services usage and transfer	services on public networks for SaaS pre-subscription **<Control: 7.3.1>** Protecting application services transactions for SaaS pre-subscription **<Control: 7.3.2>**	services on public networks during SaaS subscription **<Control: 8.3.1>** Protecting application services transactions during SaaS subscription **<Control: 8.3.2>**		
18	Application	d) Application development management	Secure development policy for SaaS pre-subscription **<Control: 7.4.1>**	Secure development policy during SaaS subscription **<Control: 8.4.1>**	Not applicable to the Subscriber	14.2.1

6 Additional Cloud Service Extended Control Set (ISO/IEC 27017:2015(E)) not covered in ISO/IEC 27036-4(E)

This section provides guidance on specific additional cloud service extended controls sets defined in the ISO/IEC 27017:2015(E) associated with each subscription stage (Pre, During and Post), (refer to Table 4).

If the control is not applicable to the Subscriber, it is recommended for the Provider to comply minimum requirements defined in the ISO/IEC 27017:2015(E) or ISO/IEC 27018:2018(E). Otherwise, the Subscriber should perform proper risk assessment to understand what risk might be present.

Table 4: Additional Cloud Service Extended Control Set

<table>
<tr><th rowspan="2">NO.</th><th rowspan="2">Additional cloud-specific information or controls in ISO/IEC 27017</th><th rowspan="2">Cloud capabilities type</th><th colspan="3">Cloud Subscription Stages</th><th>ISO/IEC 27017</th></tr>
<tr><th>Pre</th><th>During</th><th>Post</th><th>Clauses</th></tr>
<tr><td>1</td><td>Shared roles and responsibilities within a cloud computing environment</td><td>IaaS, PaaS, SaaS</td><td rowspan="3">The Subscriber should define their roles and responsibilities in their organization procedure</td><td rowspan="3">The Subscriber should be aware and know their roles and responsibilities as defined in their organization procedure</td><td rowspan="3">Not applicable to the Subscriber</td><td>CLD 6.3.1</td></tr>
<tr><td>2</td><td>Removal of cloud service customer assets</td><td>IaaS, PaaS, SaaS</td><td>Not applicable to the Subscriber</td><td>CLD 8.1.5</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Segregation in virtual computing environments</td><td>IaaS, PaaS</td><td rowspan="2">The Subscriber should define in the contract, virtual environment running on the cloud should be protected from other the Subscriber and unauthorised persons.</td><td>The Subscriber should aware, virtual environment running on the cloud should be protected from other the Subscriber and unauthorised persons.</td><td rowspan="2">Not Applicable to the Subscriber</td><td rowspan="2">CLD 9.5.1</td></tr>
<tr><td>SaaS</td><td>The Subscriber should ensure data</td></tr>
</table>

NO.	Additional cloud-specific information or controls in ISO/IEC 27017	Cloud capabilities type	Cloud Subscription Stages			ISO/IEC 27017
			Pre	During	Post	Clauses
				running on virtual environment does not contain other organization's data		
4	Virtual Machine Hardening	IaaS	In the contract, the Subscriber should ensure the virtual machines in the cloud environment should be hardened to meet business needs.	The Subscriber should implement a harden virtual machines in the cloud environment to meet business needs.	Not applicable to the Subscriber	CLD 9.5.2
		PaaS		The Subscriber should regularly check (e.g. OS patching) the hardened virtual machines in the cloud environment to meet business needs.		
		SaaS		The Subscriber should request formal evidence on Virtual machine hardening from the Provider.		

NO.	Additional cloud-specific information or controls in ISO/IEC 27017	Cloud capabilities type	Cloud Subscription Stages			ISO/IEC 27017
			Pre	During	Post	Clauses
5	Administrator's Operational Security	IaaS, PaaS, SaaS	i) The Subscriber should ensure in the contract, the Provider specify the procedures for critical operations where failure can cause unrecoverable damage to assets in the cloud environment. ii) Critical operations are: a) Installation, modification, and deletion of virtualised devices such as servers, networks and storage b) Termination procedures for cloud service usage c) Backup and restoration	i) The Subscriber should ensure the Provider procedures are applied on critical operations where failure can cause unrecoverable damage to assets in the cloud environment. ii) The Subscriber should contact the Provider for support when failure occur iii) Critical operations are: a) Installation, changes, and deletion of virtualised devices such as servers, networks and storage b) Termination procedures for cloud service usage c) Backup and restoration	Not applicable to the Subscriber	CLD 12.1.5

NO.	Additional cloud-specific information or controls in ISO/IEC 27017	Cloud capabilities type	Cloud Subscription Stages			ISO/IEC 27017
			Pre	During	Post	Clauses
6	Monitoring of Cloud Services	IaaS, PaaS, SaaS	The Subscriber should ensure in the contract that the Subscriber can request information from the Provider of the service monitoring capabilities available for each cloud service.	The Subscriber should request information from the Provider of the service monitoring capabilities available for each cloud service.	Not applicable to the Subscriber	CLD 12.4.5
7	Alignment of security management for virtual and physical networks	IaaS, PaaS, SaaS	Not applicable to the Subscriber			CLD 13.1.4

7 SaaS: Pre-Subscription Guidance

This section serves as a guidance for the Subscriber before subscribing to SaaS. The controls provided in this section should be considered in the contract.

7.1 Controls for access and user rights

7.1.1 Information access restriction for SaaS pre-subscription

The Subscriber should ensure the Provider provide menus or options on the access controls for the application (e.g. Job roles, which provides user with the permission to perform specific task).

The Subscriber should ensure the access rights in the application are defined by the Provider (e.g. read, write, delete and execute).

The Subscriber should get details on what are the other applications that can access to the application and how the access rights for that applications are managed. (e.g. Application Programming Interface, API)

The Subscriber should be aware in the contract on how the physical or logical access controls in the SaaS are isolated and managed.

7.1.2 Use of privilege utility programs for SaaS pre-subscription

The Subscriber should identify the utility programs used (e.g. anti-virus, firewall etc.).

The Subscriber should ensure the utility programs will not interfere with the cloud service.

7.2 Controls for application changes

7.2.1 Change Management for SaaS pre-subscription

The Subscriber should ensure the Provider able to provide the following before making any changes that can adversely affect the cloud service.

a) Categories of changes (e.g. change in design, version etc.).
b) Planned date and time of changes.
c) Technical description of the changes.
d) Notification on the start and the completion of the changes.

7.3 Controls for application services usage and transfer

7.3.1 Securing application services on public networks for SaaS pre-subscription

the Subscriber should ensure the Provider secure the application services on the public networks based on these aspects as listed below:

a) Confidentiality and integrity protection:

    i) The Subscriber need to ensure the transactions in the application can only be done by the authorised personnel (e.g. perform user verification).

ii) The Subscriber need to ensure the payment information in the application can only be accessed by the authorised personnel.

iii) The Subscriber need to ensure the delivery address details are clearly stated.

iv) The Subscriber need to ensure the Provider send the confirmation of receipts after the transaction.

b) Verification process:

The Subscriber need to ensure how the verification process is done for the transactions in the application (e.g. secret code).

c) Loss or duplication of transaction information:

The Subscriber need to ensure how the Provider handle the transaction information loss and duplication.

d) Application fraud protection

The Subscriber need to ensure the application is implemented with fraud protection (e.g. multi factor authentication).

7.3.2 Protecting application service transactions for SaaS pre-subscription

The Subscriber should ensure the Provider secure the application services on the public networks based on these following aspects listed below:

a) Transaction aspects:

i) The Subscriber need to ensure the user's secret authentication information are valid and verified.

ii) The Subscriber need to ensure that the transaction happens in the application remains confidential.

iii) The Subscriber need to make sure the policy defined on how the privacy of the data kept in the application is retained.

b) Encrypted communication:

The Subscriber need to ensure that the communication channel and data are encrypted during transmission.

c) Communication protocols:

The Subscriber need to ensure secure communication protocols are used in the communication.

d) Digital certificate:

The Subscriber need to ensure that the Provider use a valid digital certificate for the application.

7.4 Application development management

7.4.1 Secure development policy for SaaS pre-subscription

The Subscriber should ensure the Provider to define secure development policy based on these aspects listed below:

a) Secure data and application development repositories:

The Subscriber should ensure the Provider to secure their repositories (e.g. encryption).

b) Security in the version control:

The Provider should ensure there is a proper process to notify the Subscriber before releasing the new version.

c) Request Vulnerability Assessment & Penetration Testing (VAPT) report:

The Subscriber should ensure VAPT report for an application can be provided upon request.

7.5 Where the Subscriber data are stored for SaaS pre-subscription

Not applicable to the Subscriber .

7.6 Access to stored the Subscriber data for SaaS pre-subscription

The Subscriber need to ensure that the data can only be accessed by the Subscriber authorised personnel.

7.7 Data transmission process for SaaS pre-subscription

The Subscriber should ensure the secure transmission of the data using secure communication network protocol.

7.8 Malware protection for SaaS pre-subscription

The Subscriber should ensure the malware protection is provided (e.g. Antivirus, Anti-Spam etc.).

7.9 Access rights to the Subscriber data for SaaS pre-subscription

The Subscriber should ensure user rights in the application are defined (e.g. user permission to read, write and execute rights).

7.10 Data Log for SaaS pre-subscription

The Subscriber should ensure event log are generated based on the activities in the application (such as add data, delete data, amend data etc.) is provided by the Provider (e.g. event logs with trusted timestamping etc.).

7.11 Application layer changes for SaaS pre-subscription

The Subscriber should ensure application changes made by the Provider should be notified (e.g. update application, disable of certain functions in the application etc.).

7.12 Data retrieval during service provision for SaaS pre-subscription

The Subscriber should ensure service availability of the SaaS application are offered by the Provider is defined (refer to SLA).

7.13 Control over data during and after service provision for SaaS pre-subscription

The Subscriber should ensure data control and ownership during and after service provision is defined.

8 SaaS: During Subscription Guidance

This section serves as a guidance for the Subscriber during subscription to SaaS. All the controls provided in this section can be considered to protect the the Subscriber data.

8.1 Controls for access and user rights

8.1.1 Information access restriction during SaaS subscription

The Subscriber should ensure the Provider to manage information access control restriction on the subscription based on these aspects listed below:

a) The Subscriber should be able to use menus/options of access controls for the application.
b) The Subscriber should be able to control the access rights in the application as defined by the Provider.
c) The Subscriber should monitor the access rights for the applications are managed.
d) The Subscriber should monitor how the physical or logical access controls in the SaaS are isolated and managed, as defined in the contract.

8.1.2 Use of privilege utility programs during SaaS subscription

The Subscriber should ensure the Provider to manage privilege access control of the utility programs based on these aspects listed below:

a) The Subscriber should monitor the utility programs used (e.g. anti-virus, firewall etc.).
b) The Subscriber should monitor the use of utility programs will not interfere with the cloud service.

8.2 Controls for application changes

8.2.1 Change Management during SaaS subscription

The Provider should provide the following before making any changes that can adversely affect the cloud service.

a) Categories of changes.
b) Planned date and time of changes.
c) Technical description of the changes.
d) Notification on the start and the completion of the changes.

8.3 Controls for application services usage and transfer

8.3.1 Securing application services on public networks during SaaS subscription

The Subscriber should ensure the Provider secure the application services on the public networks based on these aspects listed below:

a) Confidentiality and integrity protection:

   i) The Subscriber should monitor the transactions in the application can only be done by the authorised personnel.

   ii) The Subscriber should monitor the payment information in the application can only be accessed by the authorised personnel.

   iii) The Subscriber should confirm the delivery address.

   iv) The Subscriber should ensure the Provider sends the transaction confirmation (e.g. successful or unsuccessful transaction confirmation).

b) Verification process:

   The Subscriber should ensure there is verification process for the transactions in the application (e.g. email verification, password, pin etc.).

c) Loss or duplication of transaction information:

   The Subscriber should monitor if there is any transaction information loss or duplication and immediately report it to the Provider for further action.

d) Application fraud protection:

   The Subscriber should verify that the application is implemented with fraud protection (e.g. login credentials, token transactions, events filtering and etc).

8.3.2 Protecting application services transactions during SaaS subscription

The Subscriber should ensure the Provider provide protection on the application services transactions based on these aspects listed below:

a) Transaction aspects:

   i) The Subscriber should check the user's secret authentication information is valid and verified.

   ii) The Subscriber should check the transaction happens in the application remains confidential.

   iii) The Subscriber should monitor the privacy of the data kept in the application is retained.

b) Encrypted communication:

   The Subscriber should ensure and monitor the communication channel and data are encrypted during transmission (e.g. SHA-256).

c) Communication protocols:

The Subscriber need to ensure secure communication protocols are used in the communication.

d) Digital certificate:

The Subscriber should ensure the Provider uses a valid digital certificate for the application.

8.4 Application development management

8.4.1 Secure development policy during SaaS subscription

The Subscriber should ensure the Provider implement secure development policy based on these aspects listed below:

a) Secure repositories:

The Subscriber should request information from the Provider on repositories security.

b) Security in the version control:

i) The Subscriber should obtain notification from the Provider on the new release of software version and ensure the new release supports their business operations.

ii) The Subscriber should be aware of the newly released/updated software version and report any bugs found to the Provider.

c) Required application security knowledge:

The Subscriber should know about application security and if not, the Subscriber should consult a third-party consultant to get advice.

d) Request Vulnerability Assessment & Penetration Testing (VAPT) report:

The Subscriber should request vulnerability assessment and penetration testing (VAPT) report from the Provider for the application.

8.5 Where the Subscriber data are stored during SaaS subscription

Not applicable to The Subscriber .

8.6 Access to stored the Subscriber data during SaaS subscription

The Subscriber should check the data can only be accessed by authorised personnel.

8.7 Data transmission process during SaaS subscription

The Subscriber should to ensure secure transmission process are used in the communication.

8.8 Malware protection during SaaS subscription

The Subscriber should check the malware protection is appropriately maintained by the Provider.

8.9 Access rights to the Subscriber data during SaaS subscription

The Subscriber should ensure confidentiality and integrity of the data through user rights is properly managed.

8.10 Data Log during SaaS subscription

The Subscriber should be able to request the events logs of the activities related to data and application from the Provider.

8.11 Application layer changes during SaaS subscription

The Subscriber should ensure any changes on the application and application changes by the Provider should be notified.

8.12 Data retrieval during SaaS subscription

The Subscriber should monitor service availability offered by the Provider is met as defined in the contract.

The Subscriber should backup all the data stored in the application to an offline medium securely stored at the Subscriber trusted site or secure site. In case of service termination or service unavailable from the Subscriber , the Subscriber shall be able to access the data through their offline backup.

8.13 Control over data during SaaS subscription

The Subscriber should monitor who can control the data, and the ownership of the data is not changed.

9 SaaS: Post Subscription Guidance

This section serves as a guidance for the Subscriber upon SaaS termination. The controls provided in this section should be considered by the Subscriber for proper termination of service.

9.1 Controls for access and user rights

9.1.1 Information on access restriction for SaaS post-subscription

The Subscriber should ensure the Provider enforce access restriction to information based on the aspects listed below:

a) Upon service termination, the Subscriber should not be able to access the application.
b) The Subscriber should ensure that the access rights for all the users are removed to avoid extra charges.

9.2 Application development management

Not applicable to the Subscriber .

9.3 Control over data for SaaS post-subscription

The Subscriber should ensure the Provider enforce control over data in SaaS based on the aspects listed below:

a) The Subscriber should ensure the Provider perform data sanitisation after termination.
b) The Subscriber should migrate all the data before termination and during termination (grace period agreed by the Subscriber and the Provider, as defined in SLA).

c) The Subscriber should ensure complete data deletion and removal from the Provider systems (including backups) with a stipulated time frame.

10 PaaS: Pre-Subscription Guidance

This section serves as a guidance for the Subscriber before subscription to PaaS. All the controls provided in this section can be considered in the contract.

10.1 Access controls (user and administrative access for both the Subscriber and the Provider)

10.1.1 User registration and deregistration for PaaS pre-subscription

The Subscriber should ensure the Provider controls on the user registration and de-registration based on the aspects listed below:

a) The Subscriber should ensure the Provider able to provide a unique user ID.

b) The Subscriber should ensure user registration and deregistration procedure is clearly defined.

10.1.2 User access provisioning for PaaS pre-subscription

The Subscriber should ensure management of access rights are clearly defined (e.g. Access control permissions). The Subscriber should perform validation test on the account provided by the Provider by sampling the access control that is relevant for PaaS functions.

10.1.3 Management of privileged access rights for PaaS pre-subscription

The Subscriber need to ensure the authentication techniques for authenticating the cloud service admin is clearly defined (e.g. multi-factor authentication, One Time Password etc.).

10.1.4 Management of secret authentication information of users for PaaS pre-subscription

The Subscriber should ensure the Provider provides management procedures for allocating secret authentication information (e.g. passwords).

The Subscriber should ensure the secret information (such as password, One Time Password etc.) are securely transmitted to The Subscriber from the Provider via secure communication (e.g. encrypted email attachment).

The Subscriber should ensure the secret information is temporary valid for certain period of time to allow the Subscriber to update/change the secret information that was created by the Provider.

10.2 Management of logging

10.2.1 Event logging for PaaS pre-subscription

The Subscriber should ensure the Provider implement event logging based on these aspects listed below:

a) The Subscriber should ensure the Provider able to provide logging capabilities.

b) The Subscriber need to ensure the requirement for event logging is clearly defined (e.g. timestamp, User ID etc.).

10.3 Controls over OS change

10.3.1 Change Management for PaaS pre-subscription

The Subscriber should ensure the Provider able to provide the following information before making any changes that can adversely affect the cloud service.

a) Categories of changes;
b) Planned date and time of changes;
c) Technical description of the changes;
d) Notification on the start and the completion of the changes.

10.4 Establishment of treatment of intellectual property rights of the Subscriber in case backup services are provided

The Subscriber should ensure the treatment of intellectual property for the data stored in the Provider backup is defined (e.g. the data is not tampered).

10.4.1 Intellectual property rights for PaaS pre-subscription

The Subscriber should consider the followings in the contract:

a) The Subscriber should ensure that only authorised and licensed products can be installed, and make sure policy of maintaining the license are defined.
b) The Subscriber need to make sure policy for disposing or transferring software is defined.

10.5 Where the Subscriber data are stored for PaaS pre-subscription

The Subscriber needs to ensure that the data can only be accessed by the authorised personnel.

10.6 Data transmission process for PaaS pre-subscription

The Subscriber should ensure the secure transmission of the data is clearly defined (e.g. using HTTPS).

10.7 Malware protection for PaaS pre-subscription

The Subscriber should ensure the malware protection is clearly defined (e.g. installed Anti-Virus, Anti-Spam).

10.8 Access rights to the Subscriber data for PaaS pre-subscription

The Subscriber should ensure the appointed the Subscriber administrator rights are clearly defined.

10.9 Data Log for PaaS pre-subscription

The Subscriber should ensure the log of data is clearly defined.

The Subscriber should ensure event log are generated based on the activities in the virtual machines (e.g. add data, delete data, amend data, install application, delete application etc.) is provided by the Provider (e.g. event logs, time stamp etc.).

10.10 The integrity of platforms for pre-subscription

The Subscriber should ensure the integrity of their platforms is clearly defined.

Integrity defined is related to source validation process on Operating System (OS) images, application installer and etc. that are used to create the virtual machine in PaaS.

10.11 Control over data during and after service provision for PaaS pre-subscription

The Subscriber should ensure data control and ownership during and after service provision is clearly defined.

11 PaaS: During Subscription Guidance

This section serves as a guidance for The Subscriber during subscription to PaaS. All the controls provided in this section can be considered to protect the Subscriber application and data.

11.1 Access controls (user and administrative access for both the Subscriber and the Provider)

11.1.1 User registration and deregistration during PaaS subscription

The Subscriber should ensure the Provider controls on user registration and deregistration are based on these following aspects listed below:

a) The Subscriber user ID is unique (e.g. The Subscriber able to perform validation test on the user ID provided by the Provider by performing registration using the same submitted user ID used previously).
b) The Subscriber should be able to use registration and deregistration functions.
c) The Subscriber should be able to request procedures on how to use the registration and deregistration functions.

11.1.2 User access provisioning during PaaS subscription

The Subscriber should be able to manage the access rights functions on the PaaS including access rights to the application installed in the virtual machines and operating system configuration.

11.1.3 Management of privileged access rights during PaaS subscription

a) Strong password authentication:

   The Subscriber should ensure the Provider enforce strong password authentication with a minimum of 8 characters containing a random combination of uppercase and lowercase letters, numbers and symbols

b) Multifactor authentication:

   The Subscriber should ensure the Provider implements at least two multi-factors authentications in their service (e.g. password with transaction authorisation code (TAC) verification).

11.1.4 Management of secret authentication information of users during PaaS subscription

The Subscriber should be able to request procedures for management of secret authentication.

11.2 Management of logging

11.2.1 Event logging during PaaS subscription

The Subscriber should ensure the Provider implement event logging based on these aspects as listed below:

a) The Subscriber should be able to provide event logging upon request.

b) The Subscriber need to verify if the Provider follows the requirement described.

11.3 Controls over OS change

11.3.1 Change Management during PaaS subscription

The Subscriber should ensure the Provider provide the following information before making any changes that can adversely affect the cloud service.

a) Categories of changes;

b) Planned date and time of changes;

c) Technical description of the changes;

d) Notification on the start and the completion of the changes.

11.4 Establishment of treatment of intellectual property rights of the Subscriber in case backup services are provided

The Subscriber should check the treatment of intellectual property for the data stored in the the Provider backup (e.g. unauthorised modification of data).

11.4.1 Intellectual property rights during PaaS subscription

a) The Subscriber should install only authorised and licensed products.

b) The Subscriber should follow policy for disposing or transferring property (e.g. data ownership).

11.5 Where the Subscriber data are stored during PaaS subscription

The Subscriber should ensure the Provider inform and update regularly on the location of data The Subscriber being stored based on these aspects listed below:

a) The Subscriber should monitor the data can only be accessed by authorised personnel.

b) The Subscriber should ensure the integrity of the data is maintained.

11.6 Data transmission process during PaaS subscription

The Subscriber should monitor the transmission of the data is secured (e.g. using latest version of TLS).

11.7 Malware protection during PaaS subscription

The Subscriber should monitor the malware protection is appropriately maintained by the Provider (e.g. Antivirus, Firewall, Intrusion Detection or Prevention System).

11.8 Data access rights during PaaS subscription

The Subscriber should properly manage access rights on who can access the data through administrator rights (e.g. user permission on read, write and execute).

11.9 Data Log during PaaS subscription

The Subscriber should be able to request the events logs of the activities related to data and application from the Provider.

11.10 The integrity of platforms during PaaS subscription

The Subscriber should ensure their platforms is not tampered by the third party (e.g. unauthorized changes of configuration in the application or operating system)

11.11 Control over data during PaaS subscription

The Subscriber should monitor who can control the data, and the ownership of the data is not changed.

The Subscriber should backup all the data stored in the application (configuration, password etc.) and virtual machine (configuration, password etc.) to an offline medium securely stored at the Subscriber trusted site or secure site. In case of service termination or service unavailable from the the Provider, the Subscriber shall be able to access the data through their offline backup.

12 PaaS: Post Subscription Guidance

This section serves as a guidance for the Subscriber upon PaaS termination. The controls provided in this section should be considered by the Subscriber for proper termination of service.

12.1 Access controls (user and administrative access for both the Subscriber and the Provider)

12.1.1 User registration and deregistration for PaaS post-subscription

The Subscriber should be able to de-register their user ID. The Subscriber should validate their user ID removal status by performing test at the login for removal confirmation.

12.1.2 User access provisioning for PaaS post-subscription

The Subscriber should not be able to manage the access rights functions.

12.1.3 Management of privileged access rights for PaaS post-subscription

The Subscriber should request evidence from the Provider on the date and duration of the expiry of privileged access rights.

12.1.4 Management of secret authentication information of users for PaaS post-subscription

The Subscriber should be able to request evidence on how secret information is being removed.

12.2 Establishment of treatment of intellectual property rights of the Subscriber in case backup services are provided

The Subscriber should ensure the data stored in the Provider backup has been completely removed and ensure the Provider perform data sanitisation.

The Subscriber should request evidence of data stored completely removed from the Provider upon request of termination and after certain period of time (upon completion of termination grace period; e.g. 3 months or 6 months).

12.2.1 Intellectual property rights for PaaS post-subscription

a) The Subscriber should install only authorised and licensed products.

b) The Subscriber should follow policy for disposing or transferring property (e.g. data ownership).

12.3 Control over data for PaaS post-subscription

The Subscriber should ensure on how the Provider manage the controls over the Subscriber data based on the following aspects as listed below:

a) The Subscriber should ensure the Provider perform data sanitisation after termination.

b) The Subscriber should migrate all the data before termination and during termination (grace period agreed by the Subscriber and the Provider, as defined in SLA).

13 IaaS: Pre-Subscription Guidance

This section serves as a guidance for the Subscriber before subscription to IaaS. All the controls provided in this section can be considered in the contract.

13.1 Controls for network security (including network access)

13.1.1 Management of privileged access rights for IaaS pre-subscription

The Subscriber should ensure the Provider to manage the access control rights and privileges (e.g. Access control permissions).

The Subscriber should perform validation test on the account provided by the Provider by sampling the access control that is relevant IaaS functions are based on the aspects as listed below.

a) Strong password authentication:

   The Subscriber should ensure the Provider enforce strong password authentication minimum of 8 characters with a random combination of uppercase and lowercase letters, numbers and symbols

b) Multifactor authentication:

   The Subscriber should ensure the Provider implements at least two multi-factors authentications on their service.

13.1.2 Segregation in Network for IaaS pre-subscription

a) The Subscriber should ensure the Provider to manage network segregation for multi-tenant access (e.g. Isolated IP segments).
b) The Subscriber should ensure the Provider manage to divide large network into separate domains based on the trust level (e.g. public access, desktop domain, server domain).

13.2 Controls for communication security (including cryptography)

The Subscriber should ensure the Provider implements cryptographic control that comply with relevant agreement, legislation and regulations.

13.2.1 Policy on the use of cryptographic controls for IaaS pre-subscription

On the use of cryptographic policy, the Subscriber should consider the followings:

a) The Subscriber policy requirements:

   The Subscriber should ensure the level of cryptographic protection for data in transit and data at rest provided by the Provider is clearly defined (e.g. list of recommended secure cryptograpghic algorithm accepted by the industry).
b) Cryptographic protection:

   The Subscriber need to ensure secure communication protocols are used.

   The Subscriber should ensure that the Provider uses encryption for data in transit and data at rest.
c) Cryptographic controls for Data in Rest and Data in Transit:

   The Subscriber should ensure cryptographic control is used by the Provider to achieve different information security objectives as described below:

   i) **Confidentiality**: To protect sensitive or critical information, either stored or transmitted.

   ii) **Integrity/authenticity**: Using digital signatures or message authentication codes to verify the authenticity or integrity of stored and transmitted sensitive or critical information.

   iii) **Non-repudiation**: Using cryptographic techniques to provide evidence of event or action.

   iv) **Authentication**: Using cryptographic techniques to authenticate the the Subscriber and other system entities requesting access to transacting with the Subscriber system, entities and resources.

13.2.2 Regulation of cryptographic controls for IaaS pre-subscription

The Subscriber should consider the following items for compliance with relevant contract, laws and regulations:

a) The Subscriber to ensure restriction on import or export of computer hardware and software.
b) The Subscriber should take advice from legal on compliance with relevant legislation and regulations before encrypted information moved across jurisdiction borders
c) The Subscriber should ensure the Provider is able to protect the Subscriber data from being access by other countries authorities through implementation of cryptographic protection.

13.3 Controls for storage security (including physical storage and security during the lifecycle)

The Subscriber should consider the following items for controls on the storage security.

a) The Subscriber should aware on where the inventory and associated assets are stored.
b) The records of inventory should indicate where the assets are maintained.
c) The Subscriber should ensure the label and associated asset information are maintained.

13.3.1 Inventory of assets for IaaS pre-subscription

The Subscriber should consider the following items for inventory assets management.

a) The Subscriber should consider inventory of assets are properly maintained.
b) The Subscriber should consider the lifecycle includes creation, processing, storage, transmission, deletion and destruction of assets.
c) The Subscriber should consider the asset inventory is accurate, up to date, consistent and aligned with other inventories.

13.3.2 Labelling of information for IaaS pre-subscription

The Subscriber should consider the following items assets labelling management.

a) The Subscriber should ensure labelling covers both physical and electronic format.
b) The Subscriber should ensure the labels are easily recognised.
c) The Subscriber should consider how the assets are handled based on the type of media.

13.3.3 Removal of the Subscriber assets for IaaS pre-subscription

As for the Assets removal agreement on termination, the Subscriber should consider the following actions.

a) The Subscriber should be able to request a documented description on the termination of service process that covers return and removal of the Subscriber assets.
b) The Subscriber should ensure all copies are deleted from the Provider systems upon termination.
c) The Subscriber should ensure the Provider should be able to provide a documented list of all the assets and service termination schedule.

13.4 Malware protection

The Subscriber should have an awareness on implementation, detection, prevention and recovery to protect against malware.

13.4.1 Controls against malware for IaaS pre-subscription

In protection against malware, the Subscriber should consider the followings:

a) The Subscriber should establish a formal policy to prohibit the use of unauthorised software.

b) The Subscriber should Implement controls that prevent or detect unauthorised software (e.g. Firewall).

c) The Subscriber should Implement control that prevents or detect known or suspected malicious websites (e.g. Blacklisting sites).

d) The Subscriber should ensure external network or on any other medium is free from malware (e.g. Trusted networks).

e) The Subscriber should conduct regular reviews on the software and data.

f) The Subscriber should install and applied regular update for malware detection (e.g. Antivirus).

g) The Subscriber should repair software through routine basis scanning on computers and media (e.g. file, electronic mail attachment and web pages).

h) The Subscriber should prepare appropriate business continuity plans for recovering from malware attack.

13.5 Monitoring

13.5.1 Clock Synchronisation for IaaS pre-subscription

The Subscriber should ensure their clock system is synchronise with the Provider Network Time Protocol (NTP) server. Without such synchronisation, it can be challenging to reconcile events on the Subscriber systems with events on the Provider systems.

13.6 Capacity management for IaaS pre-subscription

Agreement on capacity requirements for the Subscriber to be consider upon subscription with the Provider should include the following.

a) The Subscriber should ensure the agreed capacity provided by the Provider meets the The Subscriber requirements.

b) The Subscriber should identify the usage of the resources, and forecast their capacity needs, to ensure the performance of the services.

Managing capacity demands include:

a) Deletion of obsolete data.

b) Optimising batch processes and schedule.

c) Decommissioning of applications, systems, databases or environments.

d) Optimising application logic or database queries.

13.7 Identity management

Not applicable to the Subscriber .

13.8 Incident management

The Subscriber should ensure the Provider implements the Incident Management control that comply with relevant contract.

13.8.1 Incident responsibilities and procedures for IaaS pre-subscription

The Subscriber should ensure the Provider defined incident management responsibilities, incident handling procedures and incident reporting procedures.

13.8.2 Collection of evidence for IaaS pre-subscription

The Subscriber and the Provider should agree on the procedures to respond or to request for any potential evidence or other information within the cloud environment.

13.9 Establishment of treatment of intellectual property rights of the Subscriber in case backup services are provided

The Subscriber should ensure the treatment of intellectual property for the data stored in the the Provider backup is defined (e.g. the data is not tampered).

13.9.1 Intellectual property rights for IaaS pre-subscription

The Subscriber should consider the followings in the contract:

a) The Subscriber should ensure that only authorised and licensed products can be installed, and make sure policy of maintaining the license are defined.
b) The Subscriber need to make sure policy for disposing or transferring software is defined.

13.10 Where the Subscriber data are stored for IaaS Pre-subscription

The Subscriber should ensure the location of the data storage is defined (e.g. region).

13.11 Access to stored the Subscriber data for IaaS Pre-subscription

The Subscriber should ensure that the data stored can only be accessed by authorised personnel.

13.12 Control over data during and after service provision for IaaS pre-subscription

The Subscriber should ensure data control and ownership during and after service provision are defined.

14 IaaS: During Subscription Guidance

This section serves as a guidance for the Subscriber during subscription to IaaS. All the controls provided in this section can be considered to be implemented during the configuration of virtual machine.

14.1 Controls for network security (including network access)

14.1.1 Management of privileged access rights during IaaS subscription

The Subscriber should ensure the Provider manage the access control rights and privileges based on these aspects listed below:

a) Strong password authentication:

   The Subscriber should ensure the Provider enforce strong password authentication minimum of 8 characters with a random combination of uppercase and lowercase letters, numbers and symbols

b) Multifactor authentication:

The Subscriber should ensure the Provider implements at least two multi-factors authentications in their service (e.g. password with transaction authorisation code (TAC) verification).

The Subscriber should perform validation test on the account provided by the Provider by sampling the access control that is relevant IaaS functions

14.1.2 Segregation in Network during IaaS subscription

The Subscriber should ensure the Provider manage the network segregation for multi-tenants' access (e.g. Isolated IP segments, network architecture diagram etc.).

The Subscriber should ensure the Provider manage to divide large network into separate domains based on the trust level (e.g. public access, desktop domain, server domain etc.).

14.2 Controls for communication security (including cryptography)

The Subscriber should monitor, the cryptographic control that applies to the use of cloud service comply with the relevant agreement, legislation and regulations.

14.2.1 Policy on the use of cryptographic controls during IaaS subscription

On the use of cryptographic policy, the Subscriber should consider the followings:

a) The Subscriber policy requirements:

The Subscriber should ensure the level of cryptographic protection for data in transit and data at rest provided by the Provider is clearly defined (e.g. list of recommended secure cryptograpghic algorithm accepted by the industry).

b) Cryptographic protection:

The Subscriber need to ensure secure communication protocols are used.

The Subscriber should ensure that the Provider uses encryption for data in transit and data at rest

14.2.2 Regulation of cryptographic controls during IaaS subscription

a) The Subscriber should have restriction on import or export of computer hardware and software.

b) The Subscriber should take advice from legal on compliance with relevant legislation and regulations before encrypted information moved across jurisdiction borders

c) The Provider should be able to protect the Subscriber data from being access by other countries authorities through implementation of cryptographic protection.

14.3 Controls for storage security (including physical storage and security during the lifecycle)

a) The Subscriber should monitor on where the inventory and associated assets are stored.

b) The records of inventory should indicate where the assets are maintained.

c) The Subscriber should ensure the label and associated asset information are maintained properly by the Provider.

14.3.1 Inventory of assets during IaaS subscription

The Subscriber should ensure the Provider provide mechanism of inventory assets management.

a) The Subscriber should monitor that the inventory of these assets is appropriately maintained.
b) The Subscriber should monitor the lifecycle include creation, processing, storage, transmission, deletion and destruction of the asset.
c) The Subscriber should monitor asset inventory is accurate, up to date, consistent and align with other inventories.

14.3.2 Labelling of information during IaaS subscription

a) The Subscriber should ensure labelling covers both physical and electronic format.
b) The Subscriber should ensure the labels are easily recognised.
c) The Subscriber should know how the assets are handled based on the type of media.

14.3.3 Removal of the Subscriber assets during IaaS subscription

a) The Subscriber should request a documented description on the termination of service process that covers return and removal of the Subscriber assets and the Subscriber ensure that all copies are deleted from the Provider systems.
b) The Provider should be able to provide documented list of all the assets and service termination schedule upon request.

14.4 Malware protection

The Subscriber should have an awareness and monitor the implementation, detection, prevention and recovery to protect against malware during the subscription of the cloud service.

14.4.1 Controls against malware during IaaS subscription

In protection against malware, the Subscriber should consider the followings:

a) The Subscriber should have a formal policy to prohibit unauthorised software.
b) The Subscriber should Implement controls that prevent or detect unauthorised software.
c) The Subscriber should Implement control that prevents or detect known or suspected malicious websites (e.g. blacklisting sites)
d) The Subscriber ensure external network or on any other medium is free from malware (e.g. whitelisted external networks, flash drives).
e) The Subscriber should conduct regular reviews on the software and data.
f) The Subscriber should install and applied regular update for malware detection (e.g. Anti-virus).
g) The Subscriber should repair software through routine basis scanning on computers and media (e.g. file, electronic mail attachment and web pages).
h) The Subscriber should have prepared an appropriate business continuity plans for recovering from malware attack (e.g. backup).

14.5 Monitoring

14.5.1 Clock synchronization during IaaS subscription

The Subscriber should ensure their clock system is synchronised with the Provider Network Time Protocol (NTP) server.

14.6 Capacity management during IaaS subscription

In capacity management the Subscriber should demand the followings:

a) Deletion of obsolete data.
b) Optimising batch processes and schedule.
c) Decommissioning of applications, systems, databases or environments.
d) Optimising application logic or database queries.
e) The Provider provide the capacity based on the Subscriber requirements.
f) The Subscriber should identify the usage of the resources, and forecast their capacity needs, to ensure the performance of the services (e.g. scalability limit of the resource).

14.7 Identity management during IaaS subscription

Not applicable for The Subscriber .

14.8 Incident management

The Provider should implement the Incident Management control that comply with relevant contract.

14.8.1 Incident responsibilities and procedures during IaaS subscription

The Subscriber should ensure the Provider provides incident management responsibilities, incident handling procedures and incident reporting procedures.

14.8.2 Collection of evidence during IaaS subscription

The Provider should provide any potential evidence or information upon request (e.g. snapshots of virtual machine).

14.9 Establishment of treatment of intellectual property rights of the Subscriber in case backup services are provided

The Subscriber should check the treatment of intellectual property for the data stored in the Provider backup (e.g. unauthorised modification of data).

14.9.1 Intellectual property rights during IaaS subscription

The Subscriber should install only authorised and licensed products.

The Subscriber should follow policy for disposing or transferring property (e.g. data ownership).

14.10 Where the Subscriber data are stored during IaaS subscription

The Subscriber should ensure the location of the data storage (e.g. region).

14.11 Access to stored the Subscriber data during IaaS subscription

The Subscriber should ensure that the data stored can only be accessed by authorised personnel.

14.12 Control over data during IaaS subscription

The Subscriber should check on the data control and ownership during service provision.

The Subscriber should migrate all the data before termination based on grace period agreed by the Subscriber and the Provider, as defined in contract (e.g. 3 or 6 months before termination).

15 IaaS: Post Subscription Guidance

This section serves as a guidance for the Subscriber upon IaaS termination. The controls provided in this section should be considered by the Subscriber for proper termination of the service.

15.1 Controls for storage security (including physical storage and security during the lifecycle)

a) The Subscriber should backup and migrate the inventory of assets for information and associated asset stored in the cloud environment.

b) The records of inventory should indicate where the assets are maintained.

c) The Subscriber should label backup and associated assets in the cloud environment.

15.1.1 Inventory of assets for IaaS post-subscription

The Subscriber should ensure the Provider provides the access mechanism for the Subscriber to manage the inventory assets.

a) The Subscriber should migrate, backup and aware of where the inventory of these assets.

b) The Subscriber should backup and migrate the latest assets inventory, to ensure it is consistent and aligned with other inventories.

15.1.2 Labelling of information for IaaS post-subscription

The Subscriber should backup and migrate the assets which are handled depending on the type of media (e.g. physical and electronic format).

15.1.3 Removal of the Subscriber assets for IaaS post-subscription

a) The Subscriber should request the Provider on the asset's removal procedures upon termination.

b) The Subscriber should request a documented termination of service process that covers return and removal of the Subscriber assets.

c) The Subscriber should delete all their assets from the Provider system after migration.

15.2 Identity management

Not applicable for the Subscriber .

15.3 Establishment of treatment of intellectual property rights of the Subscriber in case backup services are provided

The Subscriber should ensure the data stored in the Provider backup has been completely removed and ensure the Provider performs data sanitization.

15.3.1 Intellectual property rights for IaaS post-subscription

The Subscriber should ensure the Provider provides relevant information about the intellectual property rights based on the following aspects:

a) The Subscriber should request for proof and evidence of ownership.

b) The Subscriber should request for proof or evidence on how the Provider remove the data.

c) The Subscriber should refer to the contract on the policy for disposing data.

15.4 Control over data for IaaS post-subscription

The Subscriber should ensure the Provider perform data sanitisation after termination by requesting evidence from the Provider (e.g. screenshot of virtual hard disk wipe status etc.)

The Subscriber should request evidence of data stored is completely removed from the Provider after termination (upon completion of termination grace period; e.g. 3 months or 6 months).

Bibliography

[1] ISO/IEC 27001:2013(E), Information technology - Security techniques - Information security management system - Requirements.

[2] ISO/IEC 27002:2013(E), Information technology - Security techniques - Code of practice for information security controls.

[3] ISO/IEC 27017:2015(E), Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 26002 for cloud services.

[4] ISO/IEC 27036-4:2016(E), Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services.

Acknowledgements

CyberSecurity Malaysia would like to express our appreciation and gratitude to all members who have participated tirelessly in the development of this guideline. Members of Technical Committee on Guidelines for Securing Cloud Implementation by Cloud Service Subscriber are as follows:

Ts. Dr. Solahuddin Shamsuddin	CyberSecurity Malaysia
Ts. Dr. Maslina Daud/	
Mr. Ahmad Dahari Jarno/	
Mr. Shahrin Baharom/	
Mr. Muhammad Ashraff Ruzaidi/	
Ms. Norahana Salimin/	
Ms. Indumathi Vijayakumaran/	
Ms. Niroshini Madipalan/	
Ms. Nurul Husna Khasim/	
Mr. Mohammad Firdaus Othman/	
Ms. Nurul Syahirah Aspawi	
Mr. Sanjay Willie	Astiostech Malaysia
Mr. Ab Malek Idris/	Chief Government Security Office (CGSO)
Mr. Mohd Tanazi/	
Mr. Muhammad Helmi Abu Hassan/	
Mr. Syarifuddin Palawa	
Ms. Fatin Nabiha Ab Aziz/ Ms. Nor Hashikin Rohani	Malaysian Communications And Multimedia Commission (MCMC)
Ms. Haslinda Mat Akhir/ Mr. Mohd Shahan Salim	Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
Mr. Ahmad Zulhilmi/ Mr. Kevin Cheah	Malaysian Rubber Export Promotion Council (MREPC)
Dr. Dzaharudin Mansor/	Microsoft (Malaysia) Sdn Bhd
Mr. Amran Mansor	
Mr. Ng Kang Siong	MIMOS Berhad
Mr. Mohd Fazli Azran	OWASP Organization Malaysia
Mr. Harisfazillah Jamel	SongketMail Sdn Bhd
Ms. Lyna Maharin	TeleAwan Sdn Bhd
Mr. Cheong Ket Win/	Telekom Malaysia Berhad (TM)
Mr. Iskandar Iskak/	
Mr. Meor Ahmad Khairi/	
Mr. Nuremi Abd Halim/	
Mr. Sandeep Singh Sidhu Avatar Singh/	
Mr. Stephen Ewe/	

Mr. Thaib Mustafa/ Mr. Saifulazza Sidek	
Ms. Lim Shoo Ling	The Association of Banks in Malaysia
Dr. Masita Abdul Jalil/ Prof. Madya Dr. Noraida Haji Ali	Universiti Malaysia Terengganu
Prof. Madya Dr Masnida Hj Hussin	Universiti Putra Malaysia
Dr. Lukman A Rahim	Universiti Teknologi PETRONAS