SINGAPORE STANDARDS COUNCIL

SS 584:2015+C1:2016
(ICS 35.020; 35.040; 35.240.01)

SINGAPORE STANDARD

Specification for multi-tiered cloud computing security

Incorporating Corrigendum No. 1

Published by
SPRING singapore
Enabling Enterprise

SS 584:2015+C1:2016
(ICS 35.020; 35.040; 35.240.01)

SINGAPORE STANDARD

Specification for multi-tiered cloud computing security

SPRING Singapore
1 Fusionopolis Walk
#01-02 South Tower, Solaris
Singapore 138628
Email : standards@spring.gov.sg

ISBN 978-981-4726-00-9

This Singapore Standard was approved by the Information Technology Standards Committee (ITSC) on behalf of the Singapore Standards Council of Singapore on 31 July 2015.

First published, 2013
First revision, 2015

The ITSC, appointed by the Standards Council, consists of the following members:

		Name	Capacity
Chairman	:	Mr Yap Chee Yuen	*Member, Standards Council*
Deputy Chairman	:	Mr Chak Kong Soon	*Singapore Computer Society*
Executive Secretary	:	Ms Ho Buaey Qui	*Infocomm Development Authority of Singapore*
Members	:	Assoc Prof Chan Mun Choon	*National University of Singapore*
		Mr Cheong Tak Leong	*SPRING Singapore*
		Mr Robert Chew	*Individual Capacity*
		Assoc Prof Benjamin Gan	*Singapore Management University*
		Dr Derek Kiong	*Individual Capacity*
		Mr Karl Kwan	*Singapore Polytechnic*
		Mr Lee Kee Siang	*Information Technology Management Association*
		Mr Kelvin Ng	*Nanyang Polytechnic*
		Mr Patrick Pang	*National Research Foundation*
		Mr Harish Pillay	*Internet Society (Singapore Chapter)*
		Mr Victor Tan	*Defence Science Technology Agency*
		Prof Tham Jo Yew	*Institute for Infocomm Research*
		Mr Thomas Ting	*Association of Small and Medium Enterprises*
		Mr Yow Tau Keon	*Singapore Infocomm Technology Federation*

The Cloud Computing Standards Coordinating Task Force, appointed by the ITSC and responsible for the preparation of this standard, consists of representatives from the following organisations:

		Name	Capacity
Chairman	:	Mr Robert Chew	*Member, Standards Council*
Secretary	:	Ms Ho Buaey Qui	*Infocomm Development Authority of Singapore*
Members	:	Ms Suria R Asai	*Institute of Systems Science*
		Dr Calvin Chan	*SIM University*
		Mr Chan Kin Chong	*Chairman, Security and Privacy Standards Technical Committee*
		Mr Francis Fan	*Integrated Health Information Systems Pte Ltd*
		Mr Kwa Kim Chiong	*Information Technology Management Association*
		Dr Lee Hing Yan	*Infocomm Development Authority of Singapore*
		Mr James Loo	*Information Technology Management Association*
		Mr Kelvin Ng	*Member, ITSC*
		Ms Ng Lay Ngan	*Chairman, IT Governance Technical Committee*
		Mr Harish Pillay	*Member, ITSC*

Members	:	Mr Hammad Rajjoub	*Singapore Infocomm Technology Federation*
		Mr Martin Yates	*Singapore Computer Society*

The Multi-tiered Cloud Security Working Group, appointed by the Cloud Computing Standards Coordinating Task Force to assist in the preparation of this standard, comprises the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Dr Kang Meng Chow
Deputy Convenor	:	Mr Tao Yao Sing
Members	:	Mr Chua Kim Chuan
		Prof Lam Kwok Yan
		Mr Wong Onn Chee
		Mr John Yong

The organisations in which the experts of the Working Group are involved are:

Cisco Systems, INC
Infocomm Development Authority of Singapore
MOH Holdings Pte Ltd
PrivyLink Pte Ltd
Resolvo Systems Pte Ltd

(blank page)

Contents

Page

Page

Page

Page

Page

Foreword

This Singapore Standard was prepared by the Multi-Tiered Cloud Security Working Group of the Cloud Computing Standards Coordinating Task Force under the direction of the Information Technology Standards Committee (ITSC).

Cloud computing shifts away from conventional hosting and delivery of services to utility-based consumption in both the enterprise and personal space, enabling 'everything-as-a-service'. In the midst of a cloud environment, the traditional IT security models are no longer adequate. An example would be perimeter security which has been appropriate for conventional on premise IT systems but is often inadequate for the cloud. The cloud environment shifts the ownership of security to a shared responsibility model. An example would be physical security controls of data centres, which would traditionally be operated and managed by an organisation, whereas for a cloud User, these controls now become the responsibility of the Cloud Service Provider.

This Singapore Standard aims to foster and encourage the adoption of sound risk management and security practices for cloud computing, by providing relevant cloud computing security practices and controls for cloud users, auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers to strengthen and demonstrate the cloud security controls in place, in their cloud environments.

Acknowledgement is made for the use of information from:

- Special Publication 800-145, The National Institute of Standards and Technology (NIST) Definition of Cloud Computing – Recommendation of the National Institute of Standards and Technology, September 2011 on which Clause 4 is based;
- Special Publication 800-100, Information Security Handbook: A Guide for Managers, October 2006 on which Clause 3.12 is based;
- Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organisations, Building Effective Security Assessment Plans, June 2010 on which Clauses 3.14, 3.16 and 3.19 are based;
- Special Publication 800-60 Volume I Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008 on which Tables 4 and 5 are based;
- TR31:2012 Technical Reference for Security and Service Level Guidelines for the Usage Public Cloud Computing Services.

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. SPRING Singapore shall not be held responsible for identifying any or all of such patent rights.

NOTE

1. *Singapore Standards are subject to periodic review to keep abreast of technological changes and new technical developments. The changes in Singapore Standards are documented through the issue of either amendments or revisions.*

2. *Compliance with a Singapore Standard does not exempt users from legal obligations.*

Specification for multi-tiered cloud computing security

0 Introduction

0.1 General

Cloud computing offers great potential in reducing cost and increasing flexibility to the enterprise; however wide-spread adoption is hindered for many organisations by the inability of the Information Owners (i.e. potential Cloud Service subscribers) to make informed, risk-based decisions relating to the adoption of Cloud Services.

The purpose of this standard is to lower these recognised barriers through two methodologies:

a) Employment of a multi-tiered framework allowing a single common standard to be applied by Cloud Service Providers to meet differing cloud user needs for data sensitivity and business criticality;

b) Disclosure and security reporting to improve information transparency and visibility of risks associated with the Cloud Service and security practices of the Cloud Service Providers.

This standard builds on recognised international standards, such as ISO 27001, with the added enhancement to provide Cloud Service Users with a mechanism to benchmark and tier the capabilities of Cloud Service Providers against a set of minimum baseline security requirements. This benefits the Cloud Service Users by providing assurance to the users that the provider meets accepted minimum baseline security requirements for each tier. Cloud Service Providers benefit from having a mechanism to demonstrate the security of their offerings.

0.2 Cloud computing risks

There are a variety of risks associated with the usage of cloud computing. Unlike internal technology deployments or traditional outsourcing arrangements, in cloud computing there are typically multiple parties using the same infrastructure. While multi-tenancy introduces risks to cloud users, there are other risks that shall be taken into consideration. These include risks associated with access, infrastructure, operations and governance. This standard breaks those risks into six categories as outlined in Figure 1.

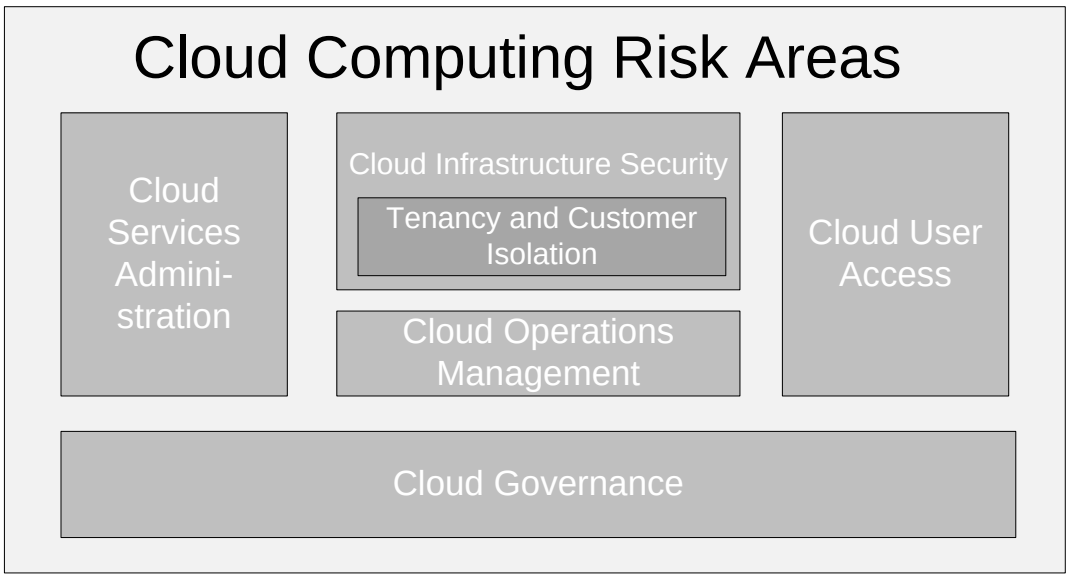

Figure 1 – Cloud computing risk areas

Cloud computing risks overlap with other Information Technology delivery models. The following areas of the standard highlight cloud computing risks that may exist in portions of existing standards like ISO 27001:

- Cloud governance;
- Cloud infrastructure security;
- Cloud operations management.

In addition, unique risks associated with cloud computing are covered in the standard:

- Cloud services administration;
- Cloud user access;
- Tenancy and customer isolation.

This standard is designed to address cloud computing risks across all of these areas as shown in Table 1.

Table 1 – Cloud computing risk areas

Cloud computing risk area	Example risks
Cloud governance	• Management not involved in overseeing Information Security for cloud computing services. • Employees not aware of appropriate usage of cloud resources. • Risk management programme does not take into account cloud risks and threats. • Third parties do not have adequately protected cloud resources. • Cloud services not consistent with legal and regulatory compliance requirements. • Insufficient processes for handling cloud incidents. • Governance of cloud data is insufficient.
Cloud infrastructure security	• Inadequate accountability and traceability of cloud usage and administration. • Cloud infrastructure is not properly configured against security threats. • Insufficient testing may not reveal security weaknesses. • Implementation and changes to systems may introduce security flaws. • Inappropriate encryption may not adequately protect sensitive data in transit and storage within the cloud environment.
Cloud operations management	• Physical environment may not support cloud security. • Inadequate management processes may not align with cloud service level requirements. • Uncontrolled changes may introduce security flaws and weaknesses. • Cloud services do not support uptime requirements.
Cloud services administration	• Intentional or unintentional actions by administrators or unauthorised individuals could affect the security of the cloud environment.
Cloud user access	• User portal has the potential to affect the security of a user's cloud instance e.g. exposing their data to unauthorised parties.
Tenancy and customer isolation	• Lack of proper segmentation between customers could expose the data and / or resources from one customer to another.

0.3 Structure

This standard specifies requirements for cloud computing security across 19 areas:

a) Core information security:

Cloud governance:

1. Information security management
2. Human resources
3. Risk management
4. Third party
5. Legal and compliance
6. Incident management
7. Data governance

Cloud infrastructure security:

8. Audit logging and monitoring
9. Secure configuration
10. Security testing and monitoring
11. System acquisition and development
12. Encryption

Cloud operations management:

13. Physical and environment security
14. Operations
15. Change management
16. Business continuity planning and disaster recovery

b) Cloud specific information security:

17. Cloud services administration
18. Cloud user access
19. Tenancy and customer isolation

The alignment of controls to common cloud service models such as IaaS, PaaS, SaaS is depicted in Table 2. The applicability of the standard is captured under Clause 1. With the diversity of specific deployments, the delineation between provider and user responsibilities may vary.

Table 2 – Alignment of controls to common cloud service models

Category	*Control category*	SaaS									User
		PaaS									User
		IaaS						User			
		Physical	*Governance*	*Network*	*Storage*	*Hardware*	*Virtualisation*	*Operating system*	*Middle ware*	*Application*	*User*
Core information security											
Cloud governance	Information security management		X								X
	Human resources		X								X
	Risk management		X								X
	Third party		X								X
	Legal and compliance		X								X
	Incident management		X								X
	Data governance		X							X	X
Cloud infrastructure security	Audit logging and monitoring			X	X	X	X	X	X	X	X
	Secure configuration			X	X	X	X	X	X		X
	Security testing and monitoring			X	X	X	X	X	X	X	X
	System acquisition and development			X	X	X	X	X	X	X	X
	Encryption			X	X	X	X	X	X	X	X
Cloud operations management	Physical and environment security	X	X								
	Operations	X		X	X	X	X	X	X	X	X
	Change management			X	X	X	X	X	X	X	X
	BCP and DR			X	X	X	X	X	X	X	X
Cloud specific information security											
Cloud services administration	Cloud services administration			X	X	X	X	X	X	X	
Cloud user access	Cloud user access				X	X	X	X	X	X	X
Tenancy and customer isolation	Tenancy and customer isolation	X	X	X	X	X	X				

This standard also includes a Cloud Service Provider Disclosure to be completed by the public Cloud Service Provider for each distinct cloud service provided. Refer to Clause 5 and Annex A for details.

0.4 Framework

Information security is the preservation of confidentiality, integrity and availability of information assets and systems (including data). This standard is based on a multi-level framework comprising three levels of information security requirements for various typical types of cloud usage, as detailed in Table 3.

Table 3 – Multi-tier cloud security framework

Level	Overview	Security control focus	Typical usage	Example data types
1	Designed for non-business critical data and systems.	Baseline security controls – "security 101" to address security risks and threats in potentially low-impact information systems using cloud services.	• Hosting web site • User control of application security • Test and Development • Simulation • Non-business critical systems	• Web site hosting public information • Data encrypted and protected from provider
2	Designed to address the needs of most organisations that run business critical data and systems.	A set of more stringent security controls required to address security risks and threats in potentially moderate-impact information systems using cloud services.	• Business critical systems	• Confidential business data • Personally Identifiable Information • Email • Customer Relationship Management (CRM) • Credit card data
3	Designed for regulated organisations with specific requirements and more stringent security requirements. Industry specific regulations may be applied in addition to these controls.	Additional set of security controls necessary to supplement and address security risks and threats in potentially high-impact information systems using cloud services.	• Hosting applications and systems with sensitive information.	• Highly confidential business data • Financial records • Medical records

0.5 Alignment of user requirements to CSP level

Users are responsible for selecting the cloud provider level, as outlined in Table 3, which best matches their specific needs and security requirements. In some cases, users may require controls above and beyond what is covered in a particular level. Consequently, they may need to select a provider at the closest level and work with the provider to ensure specific needs are addressed.

Users are advised to conduct a business impact analysis or similar self-assessment to determine the appropriate level. Typically, the higher the impact, the higher the level required as shown as follows:

- Low impact: Level 1;
- Moderate impact: Level 2;
- High impact: Level 3.

To facilitate the self-assessment, Table 4 outlines the description of the three different impact levels:

- Confidentiality: A loss of confidentiality is the unintended or unauthorised disclosure of information.
- Integrity: A loss of integrity is the unauthorised modification or destruction of information.
- Availability: A loss of availability is the disruption of access to or use of information in an information system.

Table 4 – Description of impact levels

Impact level	Description	Financial	Operational	Individuals
High	**Major damage:** Loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets, or individuals.	Major financial loss	Severe degradation in or loss of mission capability to an extent and duration that the organisation is not able to perform one or more of its primary functions.	Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate	**Significant damage:** Loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organisational operations, organisational assets, or individuals.	Significant financial loss	Significant degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.	Significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	**Minor damage:** Loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	Minor financial loss	Degradation in mission capability to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.	Minor harm to individuals.

From NIST SP 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

To provide additional context, Table 5 provides examples of the various impact types.

Table 5 – Examples of various impact types

Impact type	Examples
Financial	• Loss of sales, orders or contracts • Loss of tangible assets (e.g. fraud, theft of money, lost interest) • Penalties / legal liabilities (e.g. breach of legal, regulatory or contractual obligations) • Unforeseen costs (e.g. recovery costs) • Depressed share price (e.g. sudden loss of share value) • Delayed deliveries to customers or clients (e.g. failure to meet product delivery deadlines) • Loss of customers or clients (e.g. customer / client defection to competitors) • Loss of confidence by key institutions (e.g. adverse criticism by investors) • Damage to reputation (e.g. confidential information published in media) • Costs incurred by customers or clients (e.g. unauthorised charges)
Operational	• Loss of management control (e.g. impaired decision-making) • Loss of competitiveness (e.g. delays in the introduction of new production capabilities) • New ventures held up (e.g. delayed new products or services) • Breach of operating standards (e.g. contravention of regulatory standards)
Individuals	• Reduction in staff morale productivity (e.g. reduced efficiency) • Injury or death (e.g. harm to staff) • Loss of personal privacy data, including passwords, access tokens
From NIST SP 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories	

1 Scope

1.1 General

This standard describes the relevant cloud computing security practices and controls for public cloud users, public Cloud Service Providers, auditors and certifiers**.**

This standard covers the minimum requirements for each tier that CSPs shall meet. Additional organisation specific requirements are not within the scope of this standard.

This standard provides additional guidance for cloud users and Cloud Service Providers in Annex B and Annex C respectively.

1.2 Exclusions

This standard does not:

a) require controls to be applied to the entire organisations, rather controls can be applied to specific service offerings and the supporting infrastructure;

b) take precedence over any laws and regulations, both existing and those in the future;

c) have any legal power over the Service Level Agreements included in negotiated contracts between organisations and Cloud Service Providers;