

SS 584 : 2020
(ICS 35.020; 35.040; 35.240.01)

SINGAPORE STANDARD

Specification for multi-tiered cloud computing security

SS 584 : 2020

(ICS 35.020; 35.040; 35.240.01)

SINGAPORE STANDARD

Specification for multi-tiered cloud computing security

Published by Enterprise Singapore

All rights reserved. Unless otherwise specified, no part of this Singapore Standard may be reproduced or utilised in any form or by any means, electronic or mechanical, including photocopying and microfilming, without permission in writing from Enterprise Singapore. Request for permission can be sent to: standards@enterprisesg.gov.sg.

© Enterprise Singapore 2020

ISBN 978-981-49-2515-0

The content of this Singapore Standard was approved on 4 September 2020 by the Information Technology Standards Committee (ITSC) under the purview of the Singapore Standards Council.

First published, 2013
First revision, 2015
Second revision, 2020

The ITSC consists of the following members:

	Name	Representation
Chairman	: Mr Chak Kong Soon	<i>Individual Capacity</i>
Deputy Chairman	: Mr Harish Pillay	<i>Individual Capacity</i>
Advisor	: Mr Yap Chee Yuen	<i>Individual Capacity</i>
Secretary	: Mr Tao Yao Sing	<i>Infocomm Media Development Authority of Singapore</i>
Members	: Assoc Prof Benjamin Gan	<i>Singapore Management University</i>
	Mr Hong Tse Min	<i>Infocomm Media Development Authority of Singapore</i>
	Assoc Prof Huang Zhiyong	<i>National University of Singapore</i>
	Prof Li Xiaoli	<i>Institute for Infocomm Research</i>
	Mr Sam Liew	<i>Singapore Computer Society</i>
	Ms Lim Bee Kwan	<i>Government Technology Agency</i>
	Mr Lim Soon Chia	<i>Cyber Security Agency</i>
	Mr Kelvin Ng	<i>Nanyang Polytechnic</i>
	Mr Ong Hian Leong	<i>Individual Capacity</i>
	Mr Andy Sim	<i>SGTech</i>

ITSC set up the Technical Committee on Cloud Computing Standards to oversee the preparation of this standard. The Technical Committee consists of the following members:

	Name	Capacity
Chairman	: Mr Robert Chew	<i>Individual Capacity</i>
Secretary	: Mr Steven Tan	<i>Infocomm Media Development Authority of Singapore</i>
Members	: Dr Anton Ravindran	<i>Singapore Computer Society</i>
	Mr Chan Kin Chong	<i>Individual Capacity</i>
	Dr Calvin Chan Meng Lai	<i>Singapore University of Social Sciences</i>
	Mr Chew Weiqiang	<i>Accenture</i>
	Mr Hammad Rajjoub	<i>Individual Capacity</i>
	Dr Kang Meng Chow	<i>SGTech</i>
	Dr Ryan Ko	<i>Individual Capacity</i>
	Mr Kwa Kim Chiong	<i>Information Technology Management Association</i>
	Mr James Loo	<i>Information Technology Management Association</i>
	Mr Kelvin Ng	<i>Nanyang Polytechnic</i>

Members	:	Ms Ng Lay Ngan	<i>Institute of Systems Science</i>
		Mr Harish Pillay	<i>Individual Capacity</i>
		Mr Raju Chellam	<i>SGTech</i>
		Dr Suria P Asai	<i>Institute of Systems Science</i>
		Mr Tao Yao Sing	<i>Infocomm Media Development Authority of Singapore</i>
		Mr Wong Oon Chee	<i>Resolvo Systems</i>
		Mr Martin Yates	<i>Singapore Computer Society</i>

The Technical Committee set up the Multi-tiered Cloud Security Working Group to prepare this standard. The Working Group consists of the following experts who contribute in their *individual capacity*:

	Name
Convenor	: Dr Kang Meng Chow
Deputy Convenor	: Mr Lim Soon Chia
Members	: Dr Anton Ravindran
	Mr Mandar Bale
	Dr Ken Baylor
	Mr Chai Chin Loon
	Mr Chan Meng Fai
	Mr Dave Cheng
	Mr Chetan Sansare
	Mr Chong Jian Yi
	Mr Patrick Choong Wee Meng
	Ms Dhana Lakshmi
	Mr Gajun Ganendran
	Mr Hong Jian Hui
	Mr Lucas Kauffman
	Mr Richard Koh
	Prof Lam Kwok Yan
	Dr Lee Hing Yan
	Ms Lim May Ann
	Mr Loh Chee Keong
	Mr Manoj Wadhwa
	Mr Mok Boon Poh
	Mr Chris Ng Khee Soon
	Mr Raju Chellam
	Mr Sanjeev Gupta
	Mr Andrew Seit
	Mr Sim Bak Chor
	Mr Suresh Agarwal
	Mr Tao Yao Sing
	Ms Irene Wang

Members : Mr Wong Onn Chee
Mr Xiang Bin
Mr Zhuang Haojie

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

AliCloud
Amazon Web Services
Asia Cloud Computing Association
Association of Information Security Professionals
BSI Group Singapore Pte. Ltd.
Certification Partner Global
Cloud Security Alliance APAC
Cyber Security Agency
Ernst & Young CertifyPoint B.V.
Google Cloud
Government Technology Agency
IBM Softlayer Cloud
Infocomm Media Development Authority of Singapore
Microsoft Cloud Services
Salesforce.com
SCS Cloud Chapter
SGTech, Cloud and Data Chapter
Singapore Chinese Chamber of Commerce and Industry
SOCOTEC Certification Singapore
TÜV SÜD PSB Pte Ltd

Contents

	Page
Foreword	10
0 Introduction	11
0.1 General.....	11
0.2 Cloud computing risks	11
0.3 Structure	14
0.4 Framework	16
0.5 Alignment of user requirements to CSP level	16
1 Scope	18
1.1 General.....	18
1.2 Exclusions	18
1.3 Audience	19
2 Normative references.....	19
3 Terms, definitions and abbreviations	19
3.1 Terms and definitions.....	19
3.2 Abbreviations.....	22
4 Cloud computing fundamentals	23
4.1 Cloud computing characteristics	23
4.2 Cloud computing service models	24
4.3 Cloud computing deployment models	24
5 Other considerations	25
5.1 Applicability and compensatory controls	25
5.2 Cloud service provider disclosure	25
5.3 Considerations of emerging technologies	26
6 Information security management	27
6.1 Information security management controls	27
6.2 Information security management system (ISMS)	27
6.3 Management of information security	28
6.4 Management oversight of information security	30
6.5 Information security policy	31
6.6 Review of information security policy	32
6.7 Information security audits	32
6.8 Information security liaisons (ISL)	33
6.9 Acceptable usage	34
7 Human resources.....	35
7.1 Human resources security controls	35
7.2 Background screening	35
7.3 Continuous personnel evaluation	36
7.4 Employment and contract terms and conditions	37

7.5	Disciplinary process	38
7.6	Asset returns	39
7.7	Information security training and awareness	40
8	Risk management	41
8.1	Risk management controls	41
8.2	Risk management programme	41
8.3	Risk assessment	43
8.4	Risk management	44
8.5	Risk register	45
9	Third-party	45
9.1	Third-party security controls	45
9.2	Third-party due diligence	46
9.3	Identification of risks related to third parties	46
9.4	Third-party agreement	47
9.5	Third-party delivery management	48
10	Legal and compliance	50
10.1	Legal and compliance controls	50
10.2	Compliance with regulatory and contractual requirements	50
10.3	Compliance with policies and standards	51
10.4	Prevention of misuse of cloud facilities	52
10.5	Use of compliant cryptographic controls	53
10.6	Third-party compliance	53
10.7	Continuous compliance monitoring	54
11	Incident management	55
11.1	Incident management controls	55
11.2	Information security incident response plan and procedures	55
11.3	Information security incident response plan testing and updates	57
11.4	Information security incident reporting	58
11.5	Problem management	59
12	Data governance	60
12.1	Data governance controls	60
12.2	Data classification	60
12.3	Data ownership	61
12.4	Data integrity	61
12.5	Data labelling/handling	62
12.6	Data protection	62
12.7	Data retention	64
12.8	Data backups	65
12.9	Secure disposal and decommissioning of hardcopy, media and equipment	65
12.10	Secure disposal verification of live instances and backups	66

12.11	Tracking of data.....	67
12.12	Production data	67
13	Audit logging and monitoring	68
13.1	Audit logging and monitoring controls	68
13.2	Logging and monitoring process	68
13.3	Log review	70
13.4	Audit trails.....	70
13.5	Backup and retention of audit trails.....	71
13.6	Usage logs	72
14	Secure configuration	73
14.1	Secure configuration controls.....	73
14.2	Server and network device configuration standards	73
14.3	Malicious code prevention.....	74
14.4	Portable code	75
14.5	Physical port protection	76
14.6	Restrictions to system utilities	76
14.7	System and network session management	77
14.8	Unnecessary services and protocols	77
14.9	Unauthorised software	78
14.10	Enforcement checks.....	78
15	Security testing and monitoring	79
15.1	Security testing and monitoring controls	79
15.2	Vulnerability scanning	80
15.3	Penetration testing	81
15.4	Security monitoring	81
16	System acquisitions and development	82
16.1	System acquisitions and development security controls	82
16.2	Development, acquisition and release management.....	82
16.3	Web application security	84
16.4	System testing.....	84
16.5	Source code security.....	85
16.6	Outsourced software development	86
17	Encryption	87
17.1	Encryption and secure cryptographic key management.....	87
17.2	Encryption policies and procedures	87
17.3	Channel encryption	88
17.4	Key management	88
17.5	Electronic messaging security.....	89
18	Physical and environmental	90
18.1	Physical and environmental security controls	90

18.2	Asset management	90
18.3	Off-site movement.....	91
18.4	Physical access.....	92
18.5	Visitors.....	93
18.6	Environmental threats and equipment power failures.....	94
18.7	Physical security review	95
19	Operations	95
19.1	Operations security controls.....	95
19.2	Operations management policies and procedures	96
19.3	Documentation of service operations and external dependencies	96
19.4	Capacity management	97
19.5	Service levels	98
19.6	Reliability and resiliency.....	99
19.7	Recoverability.....	99
20	Change management	100
20.1	Change management controls	100
20.2	Change management process	100
20.3	Backup procedures	101
20.4	Back-out or rollback procedures	102
20.5	Separation of environment.....	102
20.6	Patch management procedures	103
21	Business continuity planning (BCP) and disaster recovery (DR)	104
21.1	BCP and DR controls	104
21.2	BCP framework	104
21.3	BCP and DR plans	105
21.4	BCP and DR testing	106
22	Cloud services administration.....	107
22.1	Cloud services administration controls	107
22.2	Privilege account creation	107
22.3	Generation of administrator passwords	108
22.4	Administrator access review and revocation.....	109
22.5	Account lockout.....	110
22.6	Password change.....	111
22.7	Password reset and first logon.....	111
22.8	Administrator access security	112
22.9	Administrator access logs	113
22.10	Session management	114
22.11	Segregation of duties	115
22.12	Secure transmission of access credentials	116
22.13	Third party administrative access.....	116

22.14	Service and application accounts.....	117
23	Cloud user access	118
23.1	Cloud user access controls	118
23.2	User access registration.....	118
23.3	User access security	119
23.4	User access password	120
23.5	User account lockout.....	121
23.6	User password reset and first logon change.....	122
23.7	Password protection.....	122
23.8	User session management	123
23.9	Change of cloud user's administrator details notification.....	124
23.10	Self-service portal creation and management of user accounts	125
23.11	Communication with cloud users	125
24	Tenancy and customer isolation	126
24.1	Tenancy and customer isolation controls.....	126
24.2	Multi tenancy	126
24.3	Supporting infrastructure segmentation	127
24.4	Network protection	129
24.5	Virtualisation.....	131
24.6	Storage area networks (SAN)	132
24.7	Data segregation	133
Annex A	134
Annex B	146
Bibliography	154

Foreword

This Singapore Standard was prepared by the Multi-Tiered Cloud Security Working Group set up by the Cloud Computing Standards Technical Committee under the purview of 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 service customer (CSC), these controls now become the responsibility of the Cloud Service Provider (CSP).

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 service customers, 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.

In preparing this standard, reference was made to the following publications:

- 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;
- SS ISO / IEC 21878:2019 Information technology – Security techniques – Security guidelines for design and implementation of virtualised servers.

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

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "Mature Standards". Mature Standards will not be subject to further review, unless there are requests to review such standards.*
2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*
3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Specification for multi-tiered cloud computing security

0 Introduction

0.1 General

Cloud computing offers great potential in reducing costs and increasing flexibility to an enterprise; however widespread adoption for many organisations is hindered by the inability of information owners (i.e. potential cloud service customers) 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 (CSPs) to meet differing cloud service customer 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 CSPs.

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

With the emergence of new technologies (cloud native, big data analytics, artificial intelligence (AI), machine-to-machine learning and internet of things (IoT)) and telecommunications networks with huge data bandwidth and very low latency, we envisage vast number of IoT objects, smart devices, resources and associated services in the near future. This increases in data and IoT devices with higher velocity, volume and variety, and introduces many more new cloud services. The needs to address growing security and resiliency concerns (considering new network design and edge computing protection) arising from such rapid changing environment are imminent.

0.2 Cloud computing risks

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

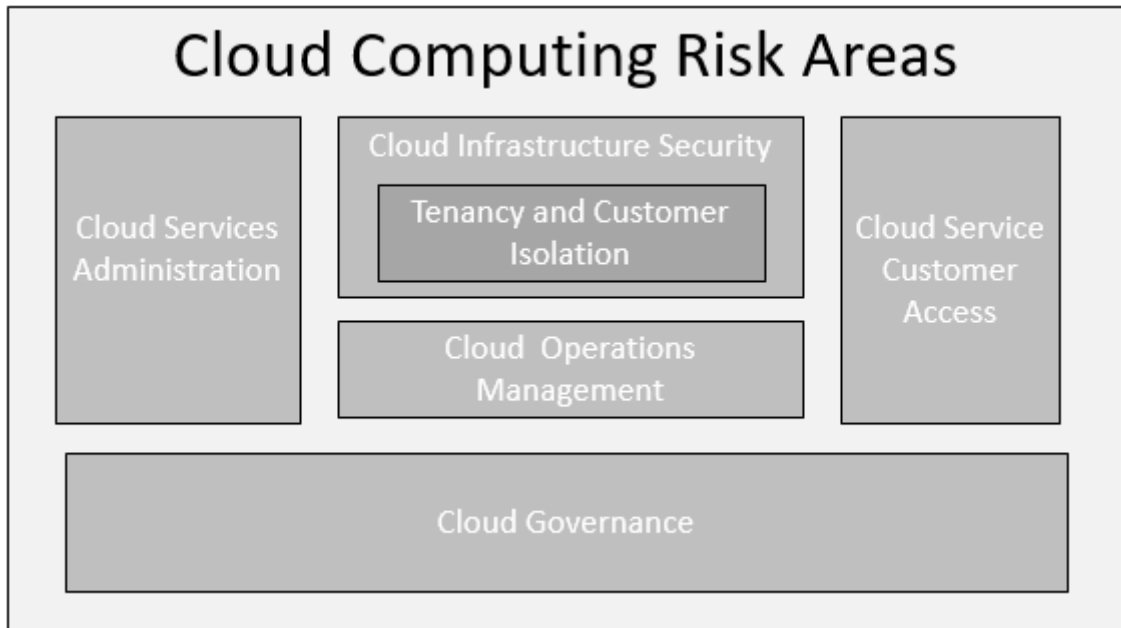


Figure 1 – Cloud computing risk areas

Cloud computing risks overlap with other information technology delivery models.

The following areas of this standard highlight cloud computing risks that may exist in portions of existing standards like ISO 27001:

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

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

- Cloud services administration;
- Cloud service customer access; and
- 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 of risks
Cloud governance	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Intentional or unintentional actions by administrators or unauthorised individuals may affect the security of the cloud environment.
Cloud service customer access	<ul style="list-style-type: none"> • Cloud service customer portal has the potential to affect the security of a cloud service customer's cloud instance (e.g. exposing their data to unauthorised parties).
Tenancy and customer isolation	<ul style="list-style-type: none"> • Lack of proper segmentation between customers may 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 (BCP) and disaster recovery (DR)

b) Cloud specific information security:

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

The alignment of controls to common cloud service models such as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS) is depicted in Table 2. The applicability of the standard is captured in Clause 1. With the diversity of specific deployments, the delineation between provider and customer's responsibilities may vary.

Table 2 – Alignment of controls to common cloud service models

Category	Control category	SaaS									Cust omer
		PaaS								Customer	
		IaaS						Customer			
		Physical	Governance	Network	Storage	Hardware	Virtualisation	Operating system	Middleware	Application	Customer
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 service customer access	Cloud service customer 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 CSP for each distinct cloud service provided. For questions not applicable or not disclosed, the public CSP shall indicate accordingly with remarks.

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 tiers of information security requirements for various typical types of cloud usage, as detailed in Table 3.

Table 3 – Multi-tiered 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.	<ul style="list-style-type: none"> • Hosting web site • User control of application security • Test and development • Simulation • Non-business critical systems 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Business critical systems 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Hosting applications and systems with sensitive information 	<ul style="list-style-type: none"> • Highly confidential business data • Financial records • Medical records

0.5 Alignment of user requirements to CSP level

Users, also commonly known as CSCs, are responsible for selecting the cloud provider level, as outlined in the previous subclause, which best matches their specific needs and security requirements. In some cases, CSCs 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.

CSCs should conduct a business impact analysis or similar self-assessment to determine the appropriate level. Typically, the higher the impact, the higher the level required:

- 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 may 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 may 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 may 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.

Based on 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Loss of management control (e.g. impaired decision-making) • Loss of competitiveness (e.g. delays in the introduction of new production capabilities) • New ventures hold-up (e.g. delayed new products or services) • Breach of operating standards (e.g. contravention of regulatory standards)
Individuals	<ul style="list-style-type: none"> • 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 CSCs, public CSPs, auditors and certifiers.

This standard covers the minimum requirements for each tier that CSPs are to meet. Additional organisation-specific requirements are not within the scope of this standard. However, for completeness of evaluation of CSPs' cloud service offerings, the standard also includes self-disclosure of non-security service-oriented parameters designed to foster transparency of key characteristics of the service with potential CSCs. The disclosure in Annex A may be used by CSCs to understand the differences amongst CSPs and evaluate how those may impact their needs.

This standard provides additional guidance for CSPs in Annex B.

1.2 Exclusions

This standard does not:

- apply controls to the entire organisations but rather controls can be applied to specific service offerings and the supporting infrastructure;
- have any legal power over the service level agreements (SLAs) included in negotiated contracts between organisations and CSPs;

- c) address requirements, legal, or otherwise, governing normal business operations to be adhered by CSPs. Examples of such requirements include detailed regulations covering building and fire safety, occupational health and safety, copyright regulations and prevailing human resource practices; and
- d) specify vendor-specific controls. Refer to vendor literature and other technical references, when necessary.

1.3 Audience

The targeted audience includes:

- a) CSPs providing IaaS, PaaS, and SaaS as part of their services;
- b) third-party service providers engaged by CSPs to support the cloud environment;
- c) public CSCs;
- d) auditors performing cloud audits; and
- e) certifiers performing cloud security assessments and providing cloud computing certifications.

CSP are certified based on the multi-level framework, comprising different levels of security requirements, as specified in this standard for each distinct service offering.

2 Normative references

The following referenced documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO / IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*