MCMC MTSFB TC G017:2021

TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - CLOUD SERVICE PROVIDERS SELECTION (FIRST REVISION)

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date : 24 August 2021

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.skmm.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Application Security Sub Working Group under the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

American Malaysian Chamber of Commerce

Celcom Axiata Berhad

Digi Telecommunications Sdn Bhd

Maxis Broadband Sdn Bhd

Telekom Malaysia Berhad

Foreword

This technical code for Information and Network Security - Cloud Service Providers Selection (First Revision) (‘this Technical Code’) was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Application Security Sub Working Group under the Security, Trust and Privacy Working Group.

This Technical Code is developed in reference to international standards such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27036-4 and other best practices on information security, cloud deployment and strategy.

Major modifications in this revision are as follows:

a) added shared responsibilities on Cloud Service Subscribers (CSS) and Cloud Service Provider (CSP) in Clause 5;

b) removed Clause 6, *Organisational assessment* and replaced with new Clause 6, *Risk assessment*;

c) rearrangement on the annexes;

d) added and modified the checklist of risk mitigation controls in Annex D;

e) moved sub-clause 7.4, *Cloud Service Provider (CSP) service reliability and performance* to Annex G; and

f) moved sub-clause 7.5, *Exit provisions* to Annex G.

This Technical Code shall replace the MCMC MTSFB TC G017:2018, *Information and Network Security - Cloud Service Providers Selection*.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INFORMATION AND NETWORK SECURITY - CLOUD SERVICE PROVIDERS SELECTION

0. Introduction

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand. Cloud computing benefits are varied and depend on the services offering. In general, cloud services provide an advantage such as self-service provisioning, elasticity, pay per use, workload resilience and migration flexibility.

A risk assessment on the security and privacy threat shall be conducted by the Cloud Service Subscribers (CSS) to further understand the specific cloud threat and common security threat. Details on common information security threat can be referred to Annex A.

The use of cloud computing has changed how organisations should assess and mitigate information and network security risks. However, unfamiliarity to shared responsibilities in the areas such as security, protection of Personally Identifiable Information (PII), regulatory compliance and governance has been identified as major concerns by potential CSS that has impeded the use of public cloud services despite being able to provide native security advantages over traditional approaches.

Cloud computing can be categorised into 3 models which are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This in turn will define the shared responsibility model for security and privacy between the Cloud Service Provider (CSP) and CSS. This Technical Code provides a high-level guideline for the selection of CSP based on risk assessment approach.

1. Scope

This Technical Code specifies requirements for organisations to select CSP to ensure all security and privacy requirements by using a risk-based approach that is structured to be generic but tailored/customised to the Communications and Multimedia Industry (CMI) requirements.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including amendments) applies.

MCMC MTSFB TC G009, *Information and Network Security - Requirements*

ISO/IEC 17788, *Information technology - Cloud computing - Overview and vocabulary*

ISO/IEC 27001, *Information Security Management*

ISO/IEC 27017, *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

ISO/IEC 27018, *Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

Act 709, *Personal Data Protection Act 2010*

General Data Protection Regulation (GDPR), European Data Protection Regulation

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex B.

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Cloud computing

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

Characteristics of cloud computing are as follows:

a) Broad network access.

b) Measured service.

c) Multi-tenancy.

d) On-demand self-service.

e) Rapid elasticity and scalability.

f) Resource pooling.

4.2 Cloud service

One or more capabilities offered through cloud computing invoked using a defined interface or any service made available to users on demand via the internet from a cloud computing provider’s server.

4.3 Cloud service customer

Party which is in a business relationship for the purpose of using cloud services.

NOTE: A business relationship does not necessarily imply financial agreements.

4.4 Cloud Service Provider (CSP)

Party which makes cloud services available.

4.5 Cloud Service Subscriber (CSS)

Equivalent to cloud service customer.

4.6 Cloud Service User (CSU)

Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE: Examples of such entities include devices and applications.

4.7 Communications and Multimedia Industry (CMI) partners

Partners of CMI such as content providers and resellers.

4.8 End points

Refers to any devices that are used to connect to the cloud services such as personal computers, mobile, Internet of Things (IoT) devices and etc.

4.9 Small enterprise

Malaysia adopted a common definition of small enterprise to facilitate identification of small enterprise in the various sectors and subsectors. This has facilitated the government to formulate effective development policies, support programmes as well as provision of technical and financial assistance. An enterprise is considered a small enterprise in each of the respective sectors based on the annual sales turnover or number of full-time employees.

5. Cloud computing service

The 6.2 of ISO/IEC 17788 defined that cloud computing offering a flexibility and various services can be used such as software, development of platforms, servers and storage over the internet. It is common to categorise cloud computing services as IaaS, PaaS and SaaS.

Details of cloud service model can be found in Annex C.

5.1 CSS and CSP responsibilities

Figure 1 illustrates the differences between CSS and CSP on their responsibilities in compliance to security and privacy requirements throughout the cloud service models offered by the CSP.

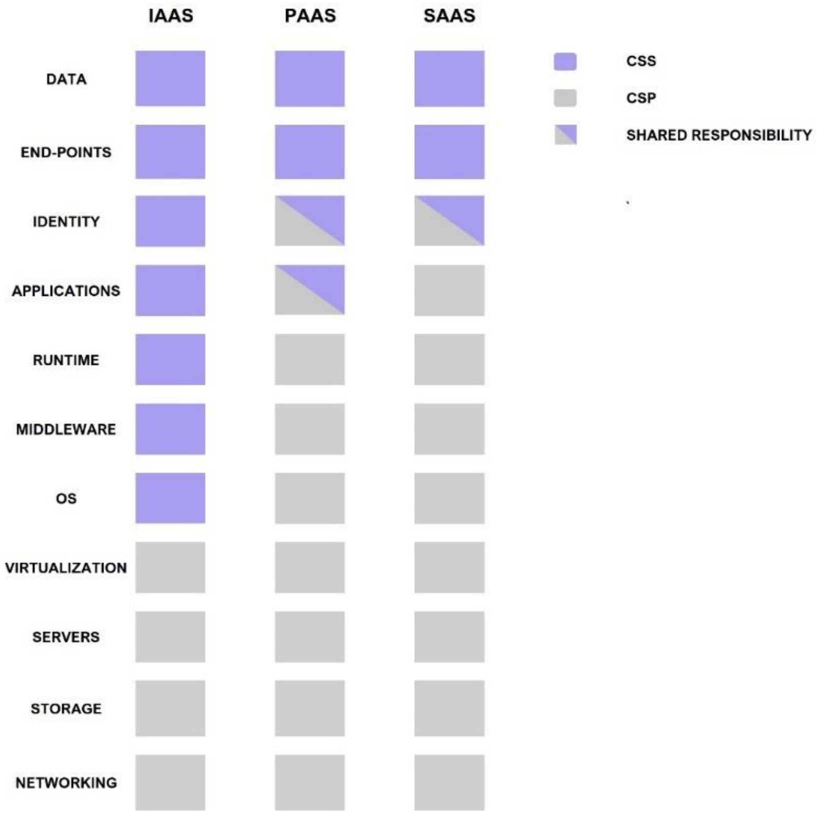
When choosing a cloud service (IaaS, PaaS, or SaaS), CSS should identify the cloud service model category. This will determine the shared responsibility model in compliance with security and privacy requirements.

For IaaS, the elements such as networking, server, storage and virtualisation will be managed by the CSP. The CSS is responsible for managing the Central Processing Unit (CPU) runtime processes, underlying Operating Systems (OS), middleware, applications, identity, end-points and data.

If CSS chosen PaaS, the management of the cloud service model would shift more to the CSP compared to the CSS. The CSS is still responsible for managing the data and endpoints while the responsibility of applications and identify is appropriately shared.

As of the CSS chosen SaaS, the responsibilities shift again. Now, the CSP is responsible for all the cloud service model management and CSS only manages the data stored in the cloud platform. The CSS is responsible for data and endpoints while identity is shared responsibility.

The virtualisation of computing and network should also apply to the CSP as well as to the CSS. Specific responsibilities for each of the cloud modelling and offering can be referred to the *Guidelines for Securing Cloud Implementation by Cloud Service Subscriber*.



	IAAS	PAAS	SAAS
DATA	🟪	🟪	🟪
END-POINTS	🟪	🟪	🟪
IDENTITY	🟪	◪	◪
APPLICATIONS	🟪	◪	⬜
RUNTIME	🟪	⬜	⬜
MIDDLEWARE	🟪	⬜	⬜
OS	🟪	⬜	⬜
VIRTUALIZATION	⬜	⬜	⬜
SERVERS	⬜	⬜	⬜
STORAGE	⬜	⬜	⬜
NETWORKING	⬜	⬜	⬜

🟪	CSS
⬜	CSP
◪	SHARED RESPONSIBILITY

Figure 1. CSP and CSS responsibilities on cloud service models

6. Risk assessment

While the benefits of adopting cloud computing offer benefits in the area of economics, agility and security compliance, it also introduces uncertainty brought about by the externalisation of Information Technology (IT) resources. This changes the risk profile for the workload. At present many organisations have yet to understand how to identify and evaluate the risks associated to cloud adoption, which in turn leads to either forego the business advantages using cloud, or using cloud in a way that introduces high security and privacy risks.

To enable the use of cloud computing in a way that properly addresses security and privacy risks, CSS shall perform a risk management approach towards selecting the CSP. This provides a formal approach to understanding and addressing the risk when considering cloud-based options and conforms to the recommendations in the MCMC MTSFB TC G009.

The following sections expand the risk management steps described in the MCMC MTSFB TC G009 for CSP selection for cloud-based IT solutions with respect to addressing security and privacy risks. The overall risk management process is not expected to be a waterfall process and should be aligned with the ISO 31000, *Risk Management,* which provides a guide to assess and evaluate the risk.

6.1 Communication and consultation

Experience has shown that leveraging cloud computing warrants a broad-based assessment set against both the IT and business objectives. This step addresses this by identifying all the stakeholders for the cloud-based IT solution and ensure that they are involved and consulted key stages in the following steps.

This would typically include~~,~~ but not limited to the following:

a) IT team;

b) business users;

c) cyber security team;

d) risk management team; and

e) legal team.

6.2 Scope, context and criteria

The scope of the cloud-based IT solution will in turn help frame the context and criteria.

The context may include but not limited to the following:

a) external context

Examples would include understanding the threat landscape and evolution, advances in cloud security, existing and new regulations and others.

b) internal context

Determine the boundaries of the system that is being developed, the existing system it interfaces with, existing Local Area Network (LAN) and Wide Area Network (WAN) and others, corporate policy and guidelines.

c) risk management context

The boundary of risks to be considered in the risk management process, which is mainly security and privacy although the process may be extended to include compliance and others.

In this stage, it is also important to agree on the following criteria:

a) criteria for identifying risks;

b) criteria for determining risks, appetite or threshold;

c) criteria for determining risk impacts; and

d) criteria for determining risk likelihood.

6.3 Risk assessment

The risk assessment process may involve the following 3 steps which may be iterative in nature.

a) Identify risk

The risk assessment stage starts with identifying all the risks that arise from security and privacy threats based on the scope, context and risk identification criteria above. This should involve a wide range of stakeholders for the targeted system. Examples of these threats that can be used as risks are provided in Annex A. In addition, there shall be consensus on determining the risk appetite for each identified risk.

b) Analyse risk

Using the criteria for determining risk impacts and likelihood, stakeholder risk impact score, and the risk likelihood should be determined and agreed upon by the stakeholders. Known compensating controls (see Annex D) could be included to reduce the impact and/or likelihood.

c) Evaluate risk

Risk evaluation will take into account both impact (the higher its impact, the higher its risks) and likelihood (the higher its likelihood, the higher its risks). Further, additional compensating controls could also be considered to reduce the risks further, while additional risks may be identified that extend the risks. Here, the risk list should then be shortened by prioritising only risks that exceed the risk threshold for the organisation.

6.4 Risk treatment

Decisions on risk treatment decisions are based on the overall risk rating and may take into account the cost of remediation. The following options may be used for risk treatment:

a) Risk reduction or elimination

   i) Having the CSP to propose solutions or explanations that reduces the risks.

   ii) The CSP successfully justifies why the risk is irrelevant.

   iii) Enterprise risk management practices to reduce probability and/or impact of the risks.

   iv) Plan for failures by defining failure counter-measures to reduce the risks.

b) Risk retention or acceptance

   i) The CSS may decide to tolerate the risk item after further consideration and/or clarification by the CSP.

c) Risk avoidance

   i) Choose not to adopt the CSP for the solution.

d) Risk transfer

   i) Cloud insurance.

   ii) Service Level Agreements (SLAs) and warranties that transfer the risks to the CSP.

6.5 Monitoring and review

At this stage, information should be available to help to compare the security and privacy risks levels for each of the candidate CSPs and determine if they meet the CSS risk tolerance thresholds. This information should be shared with the decision-makers and the other stakeholders, and further deliberation on refining the risk criteria, risk assessments, risk treatment which now may take into account cost-benefit analysis, organisational constraints, business priorities and others.

6.6 Recording and reporting risk

This involves summarising the results that will help make the final decision about the selection of the vendors. The use of modern dashboards that help a broad range of stakeholders to understand the process, the output of the analysis and comparing the capabilities side by side of the candidate CSPs may be used. This is particularly useful to obtain buy-in and non-technical stakeholders such as a board or a senior business decision maker.

7. Selection criteria

The selection criteria may vary, and at the minimum the following shall be considered:

a) Criteria for selection shall be based on the CSP which best meets the CSS risk tolerance specified during the risk management process (refer Clause 6).

   i) CSP selected for specific workload and services shall not prevent the CSS from complying to local laws and regulations such as local and international act/laws such as Act 709, *Personal Data Protection Act 2010* and *General Data Protection Regulation (GDPR)*.

   ii) CSP selected shall be able to support features that help the CSS to mitigate the risk which under CSS responsibility (refer Clause 7.1).

   iii) CSP selected may be able to support modern security architecture and methodology such as micro-segmentation, zero trust, etc.

   iv) CSP selected shall be compliant to ISO/IEC 27001 for Information Security Management System (ISMS), ISO/IEC 27017 and ISO/IEC 27018 for the cloud and privacy controls or equivalent to certifiable industry standard.

b) CSP should comply with the relevant standard and industry best practices such as:

   i) Payment Card Industry Data Security Standard (PCI DSS);

   ii) Cloud Security Alliance Cloud Controls Matrix (CSA CCM); and

   iii) ISO 22301 for Business Continuity Management System (BCMS) and resiliency.

NOTE: Refer to Annex E, for example of Cloud Control Matrix (CCM).

c) CSP selected shall be able to provide relevant certification and third-party audit report.

7.1 Data governance

The organisation shall ensure that the movement, security and privacy of the data are transparent by the implementation of the following:

a) To have a data classification and handling scheme in place that defines types of data according to sensitivity and/or policies on data residency. The data classification scheme could be reference to internal organisation data classification policy and procedures or other applicable standard data classification scheme.

b) To assess the ability to at least protect data in transit, and at rest with recognised industry practice on data encryption and cryptography.

7.2 Service dependencies and partnerships

The organisation shall be aware that CSPs may have multiple vendor relationships to support the offering services; therefore, shall select a provider that is transparent with partnership and outsourcing to the third parties.

7.2.1 CSP subcontractors and service dependencies

It is vital to disclose any service dependencies and partnerships involved in the provisioning and delivering of the cloud services.

The organisation shall ensure the following:

a) CSP shall be accountable for compliance regardless of their dependency on subcontractors; and

b) CSP shall be accountable for compliance notwithstanding the commercial transaction made via their CSP resellers.

7.2.2 CMI partners as CSS

Partners of CMI such as content providers and resellers should leverage on compliant cloud services to deliver their product and services. Their responsibility as a CSS (is shown in Figure 1) should be governed by the following to support local innovation opportunities for small enterprises in CMI.

a) Contractual obligations with CMI.

b) Contractual compliance audit to be performed by an authorised CMI auditor.

c) CMI partners should understand and be fully accountable for any of their services in supporting the CSP.

7.3 Contracts, commercials and Service Level Agreements (SLAs)

Formal agreement between the CSS and CSP is essential because it formalises the responsibilities of the relevant parties involved when a security incident occurs.

NOTE: ISO/IEC 19086-1 and ISO/IEC 19086-4 may be used as guidance when preparing the agreements.

The organisation shall ensure the following:

a) to have agreements with both parties; and

b) the contents in the agreements are understandable and do not harm or inflict huge loss to the organisation.

In preparing the agreement with the related parties, the organisation should include items in Annex F and Table G.1 as per Annex G.

Annex A
(informative)

Common information security and privacy threat

This clause lists the common key threats that directly and indirectly affect the IT environment and cloud services which are considered as a risk to the organisation. Such threats might affect the ability of a CSP to offer services, to do business, to retain customers and to avoid legal or regulatory difficulties. Threats to a given CSP will also depend on their specific service offerings and environments.

The organisations shall conduct due diligence as such a formal risk assessment which may help to identify the advantage and potential threat based on the services engagement. The benefit and threat may vary depending on the subscribed services such as IaaS, PaaS or SaaS.

The organisations shall aware of all the associated risk and threat prior to the engagement and prepare the mitigation control on each identified threat and obtain management approval.

A.1 Unauthorised administration access

The cloud computing service will include interfaces and software components that allow the CSS or organisations own staff to administer those aspects of the cloud computing service that are under the organisation’s control such as the addition or removal of organisation employee accounts, connections to the organisation’s own servers, changes to service capacity, updating the Domain Name System (DNS) entries and websites, etc.

Such administrative interfaces can become a target of choice for attackers who impersonate the organisation’s administrators to attack a CSP. Because such cloud computing services have to be accessible to the organisation’s own staff, the protection of these services becomes a major concern for cloud computing security.

A.2 Insider threats

CSPs shall consider the trustworthiness of their employees. There is always the risk of a skilled intruder successfully obtaining a position on the CSP’s data centre despite of the employee screening process.

CSP employees’ sharing administrator passwords, or otherwise leaving credentials unsecured (e.g., written on notes stuck to a screen), careless or inadequately trained users, or malicious actions by disgruntled employees will always pose a significant threat to any business.

A.3 Data breaches

Data breach is defined as the leakage of sensitive customer or organisation data to an unauthorised user, which can occur from both outside the organisation and within the organisation. Data breach from an organisation can have a huge impact on its business regarding finance, trust and loss of customers.

This may happen accidentally due to flaws in infrastructure, application design, operational issues, insufficiency of authentication, authorisation, and audit controls.

A.4 Data loss

Data loss is a sensitive matter for an organisation and can have a devastating effect on its business. Data in cloud models can be accessed by unauthorised internal employees, as well as external hackers.

Data loss mostly occurs due to malicious attack, data deletion, data corruption, loss of data encryption key, faults in the storage system, or natural disasters.

A.5 Loss of governance

In a public cloud deployment, customers cede partial control to the cloud service providers over a number of issues that may affect security. Yet cloud service agreements may not offer a commitment to resolve such issues on the part of the cloud provider, thus leaving gaps in security defences.

A.6 Inconsistency security protection

Due to decentralised architecture with different CSPs, its protection procedures may be inconsistent among security models.

A.7 Insecure Application Program Interface (API)

The security and availability of cloud services are dependent on the security of the Insecure Application Program Interface (API)'s. Weak set of APIs and interfaces can result in many security issues in the cloud. It is necessary to design these interfaces in such a way to protect from both accidental and malicious attacks.

A.8 Malware injection attack

Malware injection attack is one category of web-based attacks in which hackers exploit vulnerabilities of a web application and embed malicious codes into it that changes the course of its normal execution. The attacks included cross-site scripting, injection flaws, information leakage and improper error handling, broken authentication and session management, failure to restrict Uniform Resource Locator (URL) access, improper data validation, insecure communications, and malicious file execution.

Additional technology such as network behaviour anomaly detection should be considered while monitoring of a propriety network, and it should be used in addition to a conventional firewall and application for the detection of malware.

A.9 Account or service hijacking

Account hijacking involves the stealing of user credentials to get an access to a customer or user account, data or other computing services where the attacker can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction.

The network attacks include phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow that result in account or service hijacking.

A.10 Denial of Service (DoS)

Denial of Service (DoS) attacks are security threats that affect cloud users by preventing them from accessing hosted applications. The attack forces the cloud service to consume system resources like processing power, disk space or network bandwidth.

This type of attack can lead to a non-responsive service causing potential financial losses and damages to the reputation of the cloud provider.

Various Distributed Denial of Service (DDoS) mitigation techniques are currently in place, and the most common solution uses a clean pipe or scrubbing whereby all the traffic must pass through a cleaning pipe called "scrubbing centre" where the incoming traffic is analysed, malicious traffic is identified and blocked, and then legitimate traffic allowed to the network.

In general, the clean pipe method is more focused on defending against the volume of the traffic instead of identifying the signature and behaviour of the attack.

A.11 Malicious intent

An activity without just causes or reason to commit a wrongful act that will result in harm to another. It is intent to harm or do some damage such as brute force attack, unauthorised scanning, DNS attack and etc.

A.12 Managing privilege access

A strong process and technology on managing privilege access including recording, Two-Factor Authentication (2FA), monitoring and reviewing the access should be considered as part of the key considerations to be provided by the CSP.

Annex B
(informative)

Abbreviations

2FA	Two-Factor Authentication
A&A	Audit and Assurance
AIS	Application and Interface Security
API	Applications and Programming Interface
BCM	Business Continuity Management
BCP	Business Continuity Plan
BCR	Business Continuity Management and Operational Resilience
BIA	Business Impact Analysis
CCC	Change Control and Configuration Management
CCM	Cloud Controls Matrix
CEK	Cryptography, Encryption and Key Management
CMI	Communications and Multimedia Industry
CPU	Central Processing Unit
CSA CCM	Cloud Security Alliance Cloud Controls Matrix
CSP	Cloud Service Provider
CSS	Cloud Service Subscribers
CSU	Cloud Service User
DCS	Data Centre Security
DDoS	Distributed Denial-of-Service
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial of Service
DPIA	Data Protection Impact Assessment
DR	Disaster Recovery
DSP	Data Security and Privacy Lifecycle Management
ERM	Enterprise Risk Management
GDPR	General Data Protection Regulation
GRC	Governance, Risk and Compliance
HRS	Human Resources
HSM	Hardware Security Modules
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IoT	Internet of Things

IPY	Interoperability and Portability
ISMS	Information Security Management System
IT	Information Technology
IVS	Infrastructure and Virtualisation Security
LAN	Local Area Network
LOG	Logging and Monitoring
OS	Operating Systems
OVF	Open Virtualisation Format
PaaS	Platform as a Service
PCIDSS	Payment Card Industry Data Security Standard
PDPA	Personal Data Protection Act
PHP	Hypertext Preprocessor
PII	Personally Identifiable Information
PM	Preventive Maintenance
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SEF	Security Incident Management, E-Discovery and Cloud Forensics
SLA	Service Level Agreement
SLO	Service Level Objective
SOC2	System and Organisation Controls 2
SSL	Secure Socket Layer
SSRM	Shared Security Responsibility Model
STA	Supply Chain Management, Transparency and Accountability
TVM	Threat and Vulnerability Management
UEM	Universal Endpoint Management
URL	Uniform Resource Locator
VM	Virtual Machine
WAN	Wide Area Network
XSS	Cross Site Scripting

Annex C
(normative)

Cloud service model

There are many different types of cloud services offering, each involving different types of technology and assets. Figure C.1 indicate the application domain (which services, which assets) of a standard.

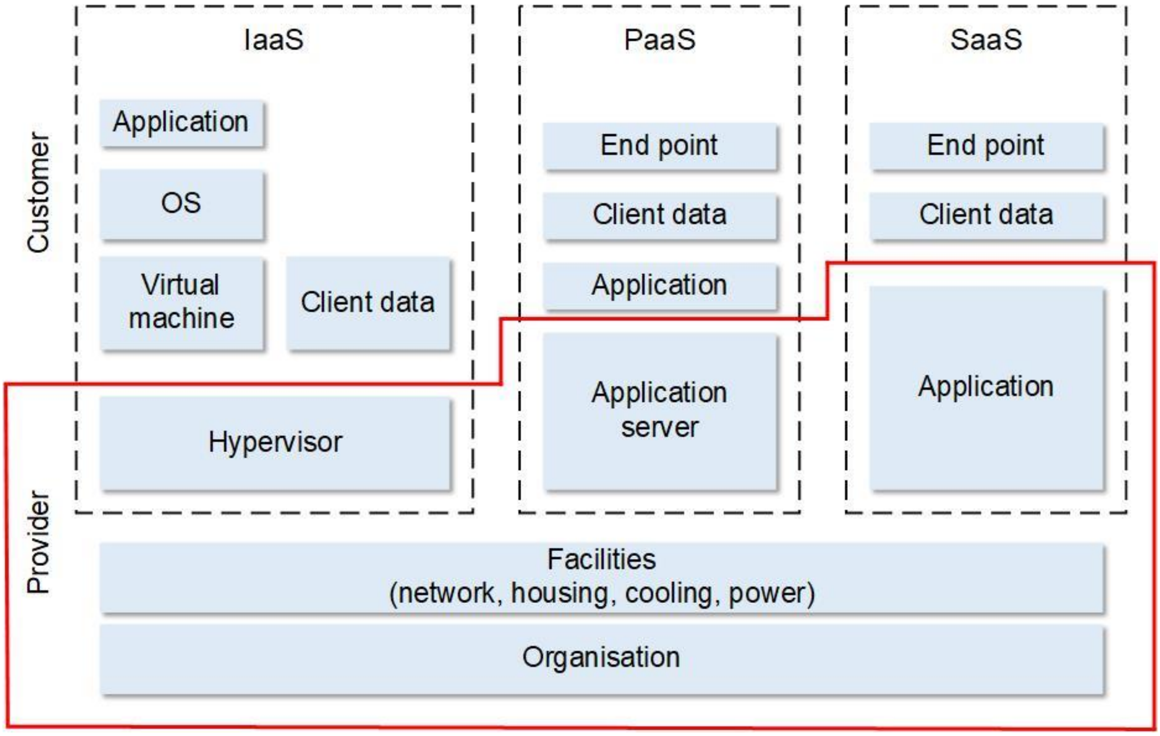


Figure C.1. Map of different technologies in the different types of cloud services

C.1 Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include OS and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over OS, storage, and deployed applications. In IaaS the provider offers storage (virtual file systems) or computing resources (virtual CPU), accessible online.

C.2 Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, OS, or storage, but has control over the deployed applications and possibly configuration settings for the application hosting environment.

In PaaS, the provider delivers a platform for customers to run applications on (often web applications). Often PaaS providers provide a software development tool to develop applications for the platform. Typical types of applications that run on these platforms are scripts (Hypertext Preprocessor (PHP), Python, etc.) or byte code (Java servlets, C#).

C.3 Software as a Service (SaaS)

The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, OS, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

In SaaS, the provider delivers full-fledged software or application via the internet. Applications range from email servers, email clients, document editors or customer relationship management systems. SaaS services can often be accessed with a browser or a web services client.

C.4 Facilities

Facilities are the basic IT resources which underline all types of cloud services (IaaS, PaaS, and SaaS), including data centre facilities such network communication, cabling and housing, cooling, fire system and power.

C.5 Organisation

Organisation are the human resources, the processes, the policies and procedures that maintain the facilities and support the delivery of services.

C.6 Deployment models

Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The relation of cloud computing is illustrated in Figure C.2.

The common deployment models are as follows:

a) Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third-party or some combination of them, and it may exist on or off premises.

b) Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

c) Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

d) Community cloud

Infrastructure provision that is exclusive to the community of consumers that have shared concerns. It may be owned by one or more organisations in the community, or a third party, or some combination of them, and it may exist on or off premises.

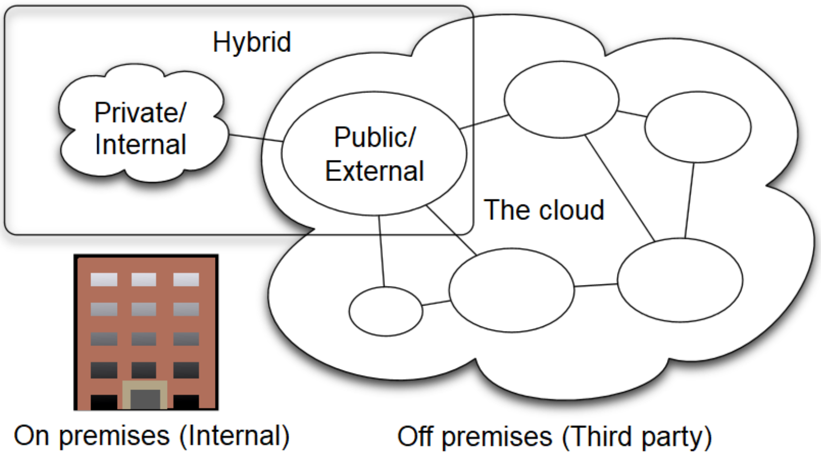


Figure C.2. Cloud computing types

The Table C.1 shows the differences between cloud deployment model according its characteristics.

Table C.1. Differences between cloud deployment model according its characteristics

Model vs characteristic	Private cloud	Public cloud	Hybrid cloud	Community cloud
Definitions (based on ISO/IEC 17788)	Cloud deployment model where cloud service are used exclusively by a single cloud service customer and resources controlled by that cloud service customer	Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider	Cloud deployment model using at least 2 different cloud deployment models	Cloud 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 collection
Cloud deployment model	Exclusively used by one CSS	Can be used by one or more CSS	Use at least 2 diferent cloud deployment models	Used by a specific collection of CSS
Cloud resource controller	CSS	Decided by the CSP	The CSP or a third party	One or more CSS in the community

Table C.1. Differences between cloud deployment model according its characteristics
(continued)

Model vs characteristic	Private cloud	Public cloud	Hybrid cloud	Community cloud
Special risk control areas	a) Security b) Privacy c) Capacity d) Business continuity e) Financial	a) Security b) Privacy c) Jurisdiction d) Concentration	a) Security b) Privacy c) Complexity d) Financial e) Interoperability	a) Security b) Privacy c) Capacity d) Business continuity e) Financial f) Governance
Security management	CSS	Joint responsibility between the CSS and CSP	Joint responsibility between the CSS and the third party controlling the resource	Joint responsibility between the CSS and, and the CSS entities controlling the resource

Annex D
(informative)

Recommended risk mitigation (controls) checklist

Table D.1. Example of compliance checklist for cloud service provider

Item	Response
The provider shall maintain formalised audit plans/reports and submit the same to organisation upon request.	
The provider shall ensure that independent reviews and assessments are performed periodically.	
The provider shall ensure that technical security assessment (including vulnerability assessment and penetration testing) of infrastructure supporting organisation is performed periodically.	
The provider shall update organisation on the agreed SLAs and security requirements periodically.	
The provider shall return and reliably erase organisation's data residing in their systems, in the event of contract expiry.	
The provider shall submit details of the locations (geographic) where organisation’s data will be stored/processed.	
The provider shall submit the details of software/applications to be installed on systems holding organisation data. The provider shall also update any risks resulting out of this and the mitigation measures deployed.	
The provider shall implement data input and output integrity routines (i.e., reconciliation and edit checks) for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	
The provider shall not be able to read/manipulate/delete any data without specific consent from organisation.	
The provider shall follow the data retention norms in line with organisation’s policies.	
The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	
The provider shall submit all structured and unstructured data related to organisation upon request in an industry-standard format (e.g. .doc, .xls, .pdf, logs, and flat files).	
The provider shall use secure (e.g., non-clear text and authenticated) and standardised network protocols for the import and export of data and to manage the service. Further, document shall be provided to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	
The provider shall use an industry-recognised virtualisation platform and standard virtualisation formats (e.g., Open Virtualisation Format (OVF)) to help ensure interoperability and shall have documented custom changes made to any hypervisor in use, available for organisation's review.	
The provider shall implement stringent physical and environmental security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) to safeguard sensitive data and information systems.	
The provider shall ensure the security at ingress and egress and any access shall be monitored by physical access control mechanisms to ensure that only authorised personnel are allowed access.	

Table D.1. Example of compliance checklist for cloud service provider *(continued)*

Item	Compliance (Y/N)
The provider shall obtain authorisation prior to relocation or transfer of hardware, software, or data to an offsite premise.	
The provider shall maintain policies and procedures for secure disposal of equipment (by asset type) used outside the organisation's premise.	
The provider shall maintain change logs for any changes made to Virtual Machine (VM) images regardless of their running state (e.g., dormant, off, or running).	
The provider shall maintain segregation/separation between the Production and non-production environments to prevent unauthorised access or changes to information assets.	
The provider shall use secured and encrypted communication channels when migrating physical servers, applications, or data to virtualised servers. Wherever possible, a network segregated from production environments shall be used for such migrations.	
The provider shall maintain a formally defined and implemented user access management process. The process should be reviewed and updated periodically.	
The provider shall restrict user access to diagnostic and configuration ports to authorised individuals and applications only.	
The provider shall maintain segregation of duties for business and operations users to ensure that conflicting functions are not assigned to same individual(s).	
The provider shall perform user access validation at planned intervals and for identified access violations. Any resulting remediation shall follow established user access policies and procedures.	
The provider shall ensure that user accounts are deleted in a timely manner in an event of user exit.	
The provider shall submit documented Business Continuity Plan (BCP) for organisation.	
The provider shall perform Business Impact Analysis (BIA) of key operational processes.	
The provider shall perform risk assessment periodically to identify, quantify and prioritise threats to information/information assets used for supporting critical processes/operations.	
The provider shall maintain escalation plan and conditions for its activation.	
The provider shall ensure that each BCP has a specific owner.	
The provider shall define roles and responsibilities for executing BCP and DRP and contact details of such users shall be communicated to interested parties (employees, contractors, third party users etc.). Further, these roles and responsibilities shall be reviewed and updated periodically.	
The provider shall demonstrate adequate physical security controls implemented at their data centre that aligned with Industry best practices.	

Annex E
(informative)

Cloud Controls Matrix (CCM)

E.1 Control domain - Audit and Assurance (A&A)

Table E.1 indicates the audit and assurance of CCM.

Table E.1. CCM - Audit and assurance

Control title	Control ID	Updated control specification
Policy and procedures	A&A-01	a) Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. b) Review and update the policies and procedures at least annually.
Independent assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.
Risk based planning assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.
Requirements compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
Audit management process	A&A-05	Define and implement an audit management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.
Remediation	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.

E.2 Control domain - Application and Interface Security (AIS)

Table E.2 indicates the application and interface security of CCM.

Table E.2. CCM - Application and interface security

Control title	Control ID	Updated control specification
Policy and procedures	AIS-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organisation's application security capabilities. b) Review and update the policies and procedures at least annually.
Application security baseline requirements	AIS-02	Establish, document and maintain baseline requirements for securing different applications.
Application security metrics	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.
Secure application design and development	AIS-04	Define and implement a Software Development Life Cycle (SDLC) process for application design, development, deployment, and operation in accordance with security requirements defined by the organisation.
Automated application security testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organisational speed of delivery goals. Automate when applicable and possible.
Automated secure application deployment	AIS-06	a) Establish and implement strategies and capabilities for secure, standardised, and compliant application deployment. b) Automate where possible.
Application vulnerability remediation	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.

E.3 Control domain - Business Continuity Management and Operational Resilience (BCR)

Table E.3 indicates the BCM and operational resilience of CCM.

Table E.3. CCM - BCM and operational resilience

Control title	Control ID	Updated control specification
BCM policy and procedures	BCR-01	a) Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. b) Review and update the policies and procedures at least annually.
Risk assessment and impact analysis	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.
Business continuity strategy	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.
BCP	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a BCP based on the results of the operational resilience strategies and capabilities.
Documentation	BCR-05	a) Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. b) Make the documentation available to authorised stakeholders and review it periodically.
Business continuity exercises	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.
Communication	BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.
Backup	BCR-08	a) Periodically backup data stored in the cloud. b) Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.
Disaster response plan	BCR-09	a) Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. b) Update the plan at least annually or upon significant changes.
Response plan exercise	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.
Equipment redundancy	BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.

E.4 Control domain - Change Control and Configuration Management (CCC)

Table E.4 indicates the change control and configuration management of CCM.

Table E.4. CCM - Change control and configuration management

Control title	Control ID	Updated control specification
Change management policy and procedures	CCC-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organisation assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). b) Review and update the policies and procedures at least annually.
Quality testing	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.
Change management technology	CCC-03	Manage the risks associated with applying changes to organisation assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).
Unauthorised change protection	CCC-04	Restrict the unauthorised addition, removal, update, and management of organisation assets.
Change agreements	CCC-05	Include provisions limiting changes directly impacting CSS owned environments/tenants to explicitly authorised requests within service level agreements between CSPs and CSS.
Change management baseline	CCC-06	Establish change management baselines for all relevant authorised changes on organisation assets.
Detection of baseline deviation	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.
Exception management	CCC-08	a) Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. b) Align the procedure with the requirements of GRC-04.
Change restoration	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.

E.5 Control domain - Cryptography, Encryption and Key Management (CEK)

Table E.5 indicates the cryptography, encryption and key management of CCM.

Table E.5. CCM - Cryptography, encryption and key management

Control title	Control ID	Updated control specification
Encryption and key management policy and procedures	CEK-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for CEK. b) Review and update the policies and procedures at least annually.
CEK roles and responsibilities	CEK-02	Define and implement CEK roles and responsibilities.
Data encryption	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.
Encryption algorithm	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.
Encryption change management	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of CEK technology changes.
Encryption change cost benefit analysis	CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.
Encryption risk management	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.
CSS key management capability	CEK-08	CSPs must provide the capability for CSS to manage their own data encryption keys.
Encryption and Key Management Audit	CEK-09	Audit encryption and key management systems, policies, and processes with frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).
Key generation	CEK-10	Generate cryptographic keys using industry-accepted cryptographic libraries specifying the algorithm strength and the random number generator used.
Key purpose	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.
Key rotation	CEK-12	Rotate cryptographic keys in accordance with the calculated crypto period, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.
Key revocation	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established crypto period, when a key is compromised, or an entity is no longer part of the organisation, which include provisions for legal and regulatory requirements.
Key destruction	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.

Table E.5. CCM - Cryptography, encryption and key management *(continued)*

Control title	Control ID	Updated control specification
Key activation	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorised for use, which include provisions for legal and regulatory requirements.
Key suspension	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.
Key deactivation	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.
Key archival	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.
Key compromise	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstances, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.
Key recovery	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.
Key inventory management	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.

E.6 Control domain - Data Centre Security (DCS)

Table E.6 indicates the data centre security of CCM.

Table E.6. CCM - Data centre security

Control title	Control ID	Updated control specification
Off-site equipment disposal policy and procedures	DCS-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organisation's premises. b) If the equipment is not physically destroyed, a data destruction procedure that renders recovery of information impossible must be applied. c) Review and update the policies and procedures at least annually.
Off-site transfer authorisation policy and procedures	DCS-02	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. b) The relocation or transfer request requires the written or cryptographically verifiable authorisation. c) Review and update the policies and procedures at least annually.
Secure area policy and procedures	DCS-03	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. b) Review and update the policies and procedures at least annually.
Secure media transportation policy and procedures	DCS-04	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. b) Review and update the policies and procedures at least annually.
Assets classification	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organisational business risk.
Assets cataloguing and tracking	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.
Controlled access points	DCS-07	a) Implement physical security perimeters to safeguard personnel, data, and information systems. b) Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.
Equipment identification	DCS-08	Use equipment identification as a method for connection authentication.
Secure area authorisation	DCS-09	a) Allow only authorised personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. b) Retain access control records on a periodic basis as deemed appropriate by the organisation.
Surveillance system	DCS-10	Implement, maintain, and operate data centre surveillance systems at the external perimeter and all the ingress and egress points to detect unauthorised ingress and egress attempts.
Unauthorised access response training	DCS-11	Train data centre personnel to respond to unauthorised ingress or egress attempts.
Cabling security	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.

Table E.6. CCM - Data centre security *(continued)*

Control title	Control ID	Updated control specification
Environmental systems	DCS-13	Implement and maintain data centre environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.
Secure utilities	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.
Equipment location	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.

E.7 Control domain - Data Security and Privacy Lifecycle Management (DSP)

Table E.7 indicates the data security and privacy lifecycle management of CCM.

Table E.7. CCM - Data security and privacy lifecycle management

Control title	Control ID	Updated control specification
Security and privacy policy and procedures	DSP-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. b) Review and update the policies and procedures at least annually.
Secure disposal	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that the data is not recoverable by any forensic means.
Data inventory	DSP-03	Create and maintain a data inventory, at least for sensitive data and personal data.
Data classification	DSP-04	Classify data according to its type and sensitivity level.
Data flow documentation	DSP-05	a) Create data flow documentation to identify what data is processed, stored or transmitted where. b) Review data flow documentation at defined intervals, at least annually, and after some change.
Data ownership and stewardship	DSP-06	a) Document ownership and stewardship of all relevant documented personal and sensitive data. b) Perform a review at least annually.
Data protection by design and default	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.
Data privacy by design and default	DSP-08	a) Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. b) Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.
Data protection impact assessment	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to applicable laws, regulations and industry best practices.
Sensitive data transfer	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorised access and only processed within scope as permitted by the respective laws and regulations.

Table E.7. CCM - Data security and privacy lifecycle management *(continued)*

Control title	Control ID	Updated control specification
Personal data access, reversal, rectification and deletion	DSP-11	Define and implement processes, procedures and technical measures to enable data subjects to request access to, modification or deletion of their personal data, according to applicable laws and regulations.
Limitation of purpose in personal data processing	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.
Personal data sub-processing	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.
Disclosure of data sub-processors	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.
Limitation of production data use	DSP-15	Obtain authorisation from data owners and manage associated risk before replicating or using production data in non-production environments.
Data retention and deletion	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.
Sensitive data protection	DSP-17	Define and implement processes, procedures and technical measures to protect sensitive data throughout its lifecycle.
Disclosure notification	DSP-18	a) The CSP must have in place and describe to CSS the procedure to manage and respond to requests for disclosure of personal data by law enforcement authorities according to applicable laws and regulations. b) The CSP must give special attention to the notification procedure to the interested CSS, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.
Data location	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.

E.8 Control domain - Governance, Risk and Compliance (GRC)

Table E.8 indicates the governance, risk and compliance of CCM.

Table E.8. CCM - Governance, risk and compliance

Control title	Control ID	Updated control specification
Governance program policy and procedures	GRC-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organisation. b) Review and update the policies and procedures at least annually.
Risk management program	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.
Organisational policy reviews	GRC-03	Review all relevant organisational policies and associated procedures at least annually or when a substantial change occurs within the organisation.
Policy exception process	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.
Information security program	GRC-05	Develop and implement an information security program, which includes programs for all the relevant domains of the CCM.
Governance responsibility model	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.
Information system regulatory mapping	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organisation.
Special interest groups	GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.

E.9 Control domain - Human Resources (HRS)

Table E.9 indicates the human resources of CCM.

Table E.9. CCM - Human resources

Control title	Control ID	Updated control specification
Background screening policy and procedures	HRS-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third-parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. b) Review and update the policies and procedures at least annually.
Acceptable use of technology policy and procedures	HRS-02	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organisationally-owned or managed assets. b) Review and update the policies and procedures at least annually.
Clean desk policy and procedures	HRS-03	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces not to have openly visible confidential data. b) Review and update the policies and procedures at least annually.
Remote and home working policy and procedures	HRS-04	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. b) Review and update the policies and procedures at least annually.
Asset returns	HRS-05	Establish and document procedures for the return of organisation-owned assets by terminated employees.
Employment termination	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.
Employment agreement process	HRS-07	Employees sign the employee agreement prior to being granted access to organisational information systems, resources and assets.
Employment agreement content	HRS-08	The organisation includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.
Personnel roles and responsibilities	HRS-09	Document and communicate roles and responsibilities of employees as they relate to information assets and security.
Non-disclosure agreements	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organisation's needs for the protection of data and operational details.
Security awareness training	HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organisation and provide regular training updates.
Personal and sensitive data awareness and training	HRS-12	Provide all employees with access to sensitive organisational and personal data with appropriate security awareness training and regular updates in organisational procedures, processes, and policies relating to their professional function relative to the organisation.
Compliance user responsibility	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory or regulatory compliance obligations.

E.10 Control domain - Identity and Access Management (IAM)

Table E.10 indicates the identity and access management of CCM.

Table E.10. CCM - Identity and access management

Control title	Control ID	Updated control specification
Identity and access management policy and procedures	IAM-01	a) Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. b) Review and update the policies and procedures at least annually.
Strong password policy and procedures	IAM-02	a) Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. b) Review and update the policies and procedures at least annually.
Identity inventory	IAM-03	Manage, store, and review the information of system identities, and level of access.
Separation of duties	IAM-04	Employ the separation of duties principle when implementing information system access.
Least privilege	IAM-05	Employ the least privilege principle when implementing information system access.
User access provisioning	IAM-06	Define and implement user access provisioning process which authorises, records, and communicates access changes to data and assets.
User access changes and revocation	IAM-07	De-provisioned or respectively modify access of movers/leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.
User access review	IAM-08	Review and revalidate user access for the least privilege and separation of duties with frequency that is commensurate with organisational risk tolerance.
Segregation of privileged access roles	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.
Management of privileged access roles	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.
CSS approval for agreed privileged access roles	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organisational risk assessment) privileged access roles.
Safeguard logs integrity	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.
Uniquely identifiable users	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.
Strong authentication	IAM-14	a) Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multi-factor authentication for at least a privileged user and sensitive data access. b) Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.

Table E.10. CCM - Identity and access management *(continued)*

Control title	Control ID	Updated control specification
Passwords management	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.
Authorisation mechanisms	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions are authorised.

E.11 Control domain - Interoperability and Portability (IPY)

Table E.11 indicates the Interoperability and portability of CCM.

Table E.11. CCM - Interoperability and portability

Control title	Control ID	Updated control specification
Policy and procedures	IPY-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: i) communications between application interfaces; ii) information processing interoperability; iii) application development portability; and iv) information/data exchange, usage, portability, integrity, and persistence. b) Review and update the policies and procedures at least annually.
Application interface availability	IPY-02	Provide application interface(s) to CSS so that they programmatically retrieve their data to enable interoperability and portability.
Secure interoperability and portability management	IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.
Data portability contractual obligations	IPY-04	Agreements must include provisions specifying CSS access to data upon contract termination and will include: a) data format; b) length of time the data will be stored; c) scope of the data retained and made available to the CSS; and d) data deletion policy.

E.12 Control domain - Infrastructure and Virtualisation Security (IVS)

Table E.12 indicates the infrastructure and virtualisation security of CCM.

Table E.12. CCM - Infrastructure and virtualisation security

Control title	Control ID	Updated control specification
Infrastructure and virtualisation security policy and procedures	IVS-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualisation security. b) Review and update the policies and procedures at least annually.
Capacity and resource planning	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.
Network security	IVS-03	a) Monitor, encrypt and restrict communications between environments to only authenticated and authorised connections, as justified by the business. b) Review these configurations at least annually and support them with a documented justification of all allowed services, protocols, ports, and compensating controls.
OS hardening and base controls	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.
Production and non-production environments	IVS-05	Separate production and non-production environments.
Segmentation and segregation	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSS (tenant) user access and intra-tenant access are appropriately segmented and segregated, monitored and restricted from other tenants.
Migration to cloud environments	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.
Network architecture documentation	IVS-08	Identify and document high-risk environments.
Network defence	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.

E.13 Control domain - Logging and Monitoring (LOG)

Table E.13 indicates the logging and monitoring of CCM.

Table E.13. CCM - Logging and monitoring

Control title	Control ID	Updated control specification
Policy and procedures	LOG-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Logging and Monitoring (LOG). b) Review and update the policies and procedures at least annually.
Audit logs protection	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.
Security monitoring and alerting	LOG-03	a) Identify and monitor security-related events within applications and the underlying infrastructure. b) Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.
Audit logs access and accountability	LOG-04	Restrict audit logs access to authorised personnel and maintain records that provide unique access accountability.
Audit logs monitoring and response	LOG-05	a) Monitor security audit logs to detect activity outside of typical or expected patterns. b) Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.
Clock synchronization	LOG-06	Use a reliable time source across all relevant information processing systems.
Logging scope	LOG-07	a) Establish, document and implement which information meta/data system events should be logged. b) Review and update the scope at least annually or whenever there is a change in the threat environment.
Log records	LOG-08	Generate an audit record containing relevant security information.
Log protection	LOG-09	The information system protects audit records from unauthorised access, modification, and deletion.
Encryption monitoring and reporting	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.
Transaction/activity logging	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.
Access control logs	LOG-12	Monitor and log physical access using an auditable access control system.
Failures and anomalies reporting	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.

E.14 Control domain - Security Incident Management, E-Discovery and Cloud Forensics (SEF)

Table E.14 indicates the security incident management, e-discovery and cloud forensics of CCM.

Table E.14. CCM - Security incident management, e-discovery and cloud forensics

Control title	Control ID	Updated control specification
Security incident management policy and procedures	SEF-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for security incident management, e-discovery, and cloud forensics. b) Review and update the policies and procedures at least annually.
Service management policy and procedures	SEF-02	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. b) Review and update the policies and procedures at least annually.
Incident response plans	SEF-03	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: a) relevant internal departments; b) impacted CSS; and c) other business critical relationships (such as supply-chain) that may be impacted.
Incident response testing	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organisational or environmental changes for effectiveness.
Incident response metrics	SEF-05	Establish and monitor information security incident metrics.
Event triage processes	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.
Security breach notification	SEF-07	a) Define and implement processes, procedures and technical measures for security breach notifications. b) Report security breaches and assume security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.
Points of contact maintenance	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

E.15 Control domain - Supply Chain Management, Transparency and Accountability (STA)

Table E.15 indicates the supply chain management, transparency and accountability of CCM.

Table E.15. CCM - Supply chain management, transparency and accountability

Control title	Control ID	Updated control specification
SSRM policy and procedures	STA-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organisation. b) Review and update the policies and procedures at least annually.
SSRM supply chain	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.
SSRM guidance	STA-03	Provide SSRM guidance to the CSS detailing information about the SSRM applicability throughout the supply chain.
SSRM control ownership	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.
SSRM documentation review	STA-05	Review and validate SSRM documentation for all cloud services the organisation uses.
SSRM control implementation	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organisation is responsible for.
Supply chain inventory	STA-07	Develop and maintain an inventory of all supply chain relationships.
Supply chain risk management	STA-08	CSPs periodically review risk factors associated with all organisations within their supply chain.
Primary service and contractual agreement	STA-09	Service agreements between CSPs and CSS (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: a) scope, characteristics and location of business relationship and services offered; b) information security requirements (including SSRM); c) change management process; d) LOG capability; e) incident management and communication procedures; f) right to audit and third-party assessment; g) service termination; h) interoperability and portability requirements; and i) data privacy
Supply chain agreement review	STA-10	Review supply chain agreements between CSPs and CSS at least annually.
Internal compliance testing	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.
Supply chain service agreement compliance	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.
Supply chain governance review	STA-13	Periodically review the organisation's supply chain partners' IT governance policies and procedures.
Supply chain data security assessment	STA-14	Define and implement a process for conducting security assessments periodically for all organisations within the supply chain.

E.16 Control domain - Threat and Vulnerability Management (TVM)

Table E.16 indicates the threat and vulnerability management of CCM.

Table E.16. CCM - Threat and vulnerability management

Control title	Control ID	Updated control specification
TVM policy and procedures	TVM-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritise the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. b) Review and update the policies and procedures at least annually.
Malware protection policy and procedures	TVM-02	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. b) Review and update the policies and procedures at least annually.
Vulnerability remediation schedule	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.
Detection updates	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly or more frequent basis.
External library vulnerabilities	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open-source libraries according to the organisation's vulnerability management policy.
Penetration testing	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.
Vulnerability identification	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organisationally managed assets at least monthly.
Vulnerability prioritization	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.
Vulnerability management reporting	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that include stakeholder notification.
Vulnerability management metrics	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.

E.17 Control domain - Universal Endpoint Management (UEM)

Table E.17 indicates the universal endpoint management of CCM.

Table E.17. CCM - Universal endpoint management

Control title	Control ID	Updated control specification
Endpoint devices policy and procedures	UEM-01	a) Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. b) Review and update the policies and procedures at least annually.
Application and service approval	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organisation-managed data.
Compatibility	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with OS and applications.
Endpoint inventory	UEM-04	Maintain an inventory of all endpoints used to store and access company data.
Endpoint management	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit or process organisational data.
Automatic lock screen	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.
OS	UEM-07	Manage changes to endpoint OS, patch levels, and/or applications through the company's change management processes.
Storage encryption	UEM-08	Protect information from unauthorised disclosure on managed endpoint devices with storage encryption.
Anti-malware detection and prevention	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.
Software firewall	UEM-10	Configure managed endpoints with properly configured software firewalls.
Data loss prevention	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.
Remote locate	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.
Remote wipe	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.
Third-party endpoint security posture	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organisational assets.

Annex F
(informative)

Service Level Agreement (SLA) responsibilities

F.1 Security

Consumer shall understand his security requirements and what controls and federation patterns are necessary to meet those requirements. A provider shall understand what they shall deliver to the consumer to enable the appropriate controls and federation patterns. The details of access control policies should be specified.

F.2 Data encryption

Data shall be encrypted while it is in motion and while it is at rest and in use. The details of the encryption algorithms and access control policies should be specified.

F.3 Privacy

Basic privacy concerns are addressed by requirements such as data encryption, retention, and deletion. An SLA should make it clear how the cloud provider isolates data and applications in a multi-tenant environment.

F.4 Data retention, deletion

Provider to prove their compliance with retention laws and deletion policies.

F.5 Hardware erasure, destruction

Provider to prove their compliance with retention laws and deletion policies.

F.6 Regulatory compliance

If regulations shall be enforced because of the type of data, the cloud provider shall be able to prove his compliance.

F.7 Transparency

For critical data and applications, providers shall be proactive in notifying consumers when the terms of the SLA are breached. This includes infrastructure issues like outages and performance problems as well as security incidents.

F.8 Certification

The provider should be responsible for proving the required certification and keeping it current.

F.9 Performance definitions

The performance definition should be agreed between CSS and CSP and should be clearly documented in the statement of work or in the contract.

F.10 Monitoring

For issues of potential breaches, you might want to specify a neutral third-party organisation to monitor the performance of the provider.

F.11 Auditability

Because the consumer is liable for any breaches that occur with loss of data or availability, it is vital that the consumer be able to audit the provider's systems and procedures. The SLA should make it clear how and when those audits take place. They can be disruptive and costly to the provider.

F.12 Metrics

These are the tangible things that can be monitored as they happen and audited after the fact. The metrics of an SLA shall be objectively and unambiguously defined. Following this list is a list of common metrics.

F.13 Providing a machine-readable SLA

This can allow for an automated, dynamic selection of a cloud broker. In other words, if your SLA requires that the broker use the cheapest possible provider for some tasks but the most secure provider for others, this type of automation makes it possible. (This type of service is not readily available yet but is something to keep in mind when contributing to the cloud SLA standardisation discussion.)

F.14 Human interaction

On demand self-service is one of the basic characteristics of cloud computing, but your SLA should take into account that when you need a human being, one is made available to you.

Organisation with critical data needs may not be satisfied with off-the-shelf agreements, so a first step before going to the cloud, the organisation should determine how critical the data and applications are. Public clouds often offer a non-negotiable SLA which may not be acceptable for those with mission critical apps or data.

An SLA contains Service Level Objectives (SLOs) that define objectively measurable conditions for the service; some examples include parameters of throughput and data streaming frequency and timing, availability percentages for VMs and other resources and instances, or urgency ratings to rank the importance of different SLOs (i.e. ‘availability is more important than response time’). SLO expectations should vary depending on whether applications and data the applications access are hosted on the same cloud or on different ones.

SLOs typically cover the following:

a) accessibility;

b) service availability (usually uptime as a percentage);

c) service capacity (what is the upper limit in terms of users, connections, resources, etc.); and

d) response time and elasticity (or how quickly changes can be accommodated).

There are often others depending on how terms are distributed between the contract and SLA.

Therefore, the organisation shall ensure the following:

a) Make sure that the SLAs shall include the following major components, but not limited to:

   i) business level and SLOs, where an organisation shall define why it will use the cloud services before it can define exactly what services it will use;

   ii) remediation policies and penalties/incentives related to these objectives; and

   iii) exclusions and caveats.

b) Check the SLOs.

c) Look for SLOs that are relevant, explicit, measurable and unambiguous. They shall also be auditable if possible and clearly articulated in the service level agreement.

d) SLAs shall also specify how issues should be identified and resolved, by who and in what time period. They will also specify what compensation is available and the processes for logging and claiming, as well as listing terms that limit the scope of the SLA and list exclusions and caveats.

e) Close scrutiny of these terms is important, as often service credit calculations are complex; ask for worked examples or give all shortlist providers the same imaginary downtime scenario and compare the difference in compensation.

Annex G
(informative)

Terms of agreement

G.1 Terms of agreement

Table G.1 indicates the terms of agreement.

Table G.1. Terms of agreement

No.	Main terms	Contents	Descriptions
1.	Service delivery	a) Clear definition of the services and deliverables. b) Clear roles and responsibilities relating to the service (delivery, provisioning, service management, monitoring, support, escalations, etc.) and how that is distributed between the customer and provider.	a) Agree on the scope of work, roles and responsibilities of the service and deliverables and how that is distributed between the customer and provider; b) confirm how service accessibility and availability is managed and assured (maintenance, incident remediation, disaster recovery, etc.); and c) ensure the agreement align with the organisation requirements.
2.	Service accessibility and availability	The maintenance, incident remediation, Disaster Recovery (DR), etc. of the service provided.	a) The capability of incident management; b) validation of BCP/DR readiness; and c) the maintenance of systems conducted regularly (Preventive Maintenance (PM), patches, upgrade, drill, etc.). d) CSP shall inform any security breach in a timely manner for the component of services under CSP responsibility.
3.	Business terms	a) Insurance policies, guarantees and penalties that are included and what caveats accompany them. b) Provision to audit (subject to CSS acceptance).	a) Check the contractual and service governance, including to what extent the provider can unilaterally change the terms of service or contract; b) ensure the clause on contract renewals and exit or modification notice periods; c) confirm the insurance policies, guarantees and penalties that are included and what caveats accompany them; d) ensure to what extent the provider is willing to expose their organisation to auditing operations and compliance to policies; and e) ensure only reputational CSPs which become the industry leader in providing and delivering cloud services.

Table G.1. Terms of agreement *(continued)*

No	Main terms	**Contents**	**Descriptions**
4.	Legal protections	Specific terms related to indemnification, IP rights, limitation of liability and warranties.	Know the specific clause relating to indemnification, IP rights, limitation of liability and warranties. They shall be standard terms in CSPs' contracts. However, the parameters relating to each of them should be scrutinised and to be mutually agreed by both parties.
5.	SLA	Cover elements such as the accessibility, service availability (usually uptime as a percentage), service capacity (what is the upper limit in terms of users, connections, resources, etc.), response time and elasticity (or how quickly changes can be accommodated). NOTE. The SLA may vary and subject to services engagement that require CSS to negotiate and agree with CSPs. For the SLA responsibilities, refer to Annex F.	a) The scope of services the CSP will deliver and a complete definition of each service; b) service delivery Metrics and auditing mechanism; c) responsibilities of both parties and remedies available to both if the terms of the SLA are not met; and d) a description of how the SLA will change over time. SLAs may be in 2 types: a) off-the-shelf agreements and customised; or b) negotiated agreements.
6.	Cyber security clause	a) To comply with relevant information security policy, process and procedures, including the confidentiality, integrity and availability of data. b) To comply with relevant regulatory and legal standard such as PDPA, PCIDSS, MCMC and other applicable regulatory and law (local and international) c) For example, of terms of service and security and privacy policy, refer to Annex H.	Data policies can be related to access, usage and others, which need to be protected by CSP. In ensuring the data policies and its protection, the organisation should review the following: a) review CSP's security policies and data management policies particularly relating to data privacy regulations; b) ensure there are sufficient guarantees around data access, data location and jurisdiction, including confidentiality, integrity and availability of data; c) scrutinise backup and resilience provisions; and d) review data conversion/disposal policies in the event of contract termination.
7.	Protection of PII	To comply with ISO 19086-4 and internal best practice to ensure sufficient protection for PII data.	

G.2 CSP service reliability and performance

The organisation shall ensure CSP can provide reliability in their service performance. The following may be used to measure the reliability of a service provider:

a) ensure the chosen CSP has established, documented and proven processes for dealing with planned and unplanned downtime, including communication with customers; and

b) be aware of remedies and liability limitations offered by the CSP when service issues arise.

G.2.1 Disaster Recovery (DR)

The organisation shall assess the following in ensuring the CSP is reliable in performing and executing during an incident:

a) the CSS and CSP's shall discuss disaster recovery provisions, processes and their ability to support the organisation's data preservation expectations (inclusive recovery time objectives and recovery point objectives). This includes critical data, data sources, scheduling, backup, restore, integrity checks, etc.;

b) the CSP's possess a clearly documented roles and responsibilities and escalation processes; and

c) consider purchasing additional risk insurance if the costs associated with recovery are not covered by the provider's umbrella terms and conditions (i.e., cybersecurity insurance).

G.2.2 Monitoring and measurement

The organisation shall monitor the performance of the CSP through tangible metrics to prevent potential breaches. The metrics shall be stated in SLA and objectively defined.

Some of the common performance metrics, which may be considered, are as follows:

a) throughput to measure the system response speed;

b) reliability to measure system availability;

c) system availability;

d) latency;

e) load balance;

f) durability to measure how likely to lose data;

g) elasticity to measure how much a resource can grow;

h) linearity to measure system performance as the load increases;

i) agility to measure how quickly the provider responds to load changes;

j) automation to measure the percent of requests handled without human interaction; and

k) customer service response times.

G.3 Exit provisions

Exit provision is an exit strategy, or a contingency plan that is executed by a business owner/CSS to terminate the service contract. The organisation shall ensure the following when preparing the transition plan:

a) to have a clear exit strategy in the contract;

b) review contract clauses, if any, during the execution of the exit plan;

c) backup, removal and transfer of data from the CSP upon exit;

d) revoke all access which related to subscribed services;

e) return hardware/software if applicable;

f) clear demarcation of IP/branding ownership; and

g) relevant data container and agree on format of data as part of the handover.

Annex H

(informative)

Example of terms of service and security and privacy policy

H.1 Terms of service and security and privacy policy

Read the terms of service and security and privacy policy by focusing on the following items:

a) how your company can use the cloud service (i.e., acceptable usage policies, licensing rights or usage restrictions);

b) how your data is stored and protected;

c) whether the service provider has access to your data, and if so, how that access is restricted;

d) how to report an incident;

e) how to terminate the service and if data is retained after service termination;

f) whether the service provider will give advance notice of any change of terms;

g) whether the privacy policy follows the data protection principles of the Personal Data (Privacy) Ordinance; and

h) the jurisdiction that the terms would apply.

Negotiate the terms of service with the service provider if not all the terms are found acceptable. If you cannot find a service provider meeting your requirements, you should re-consider the use of cloud services.

Understand whether there are secondary uses of your account information without your knowledge or consent. For example, information stored in the cloud may be used to tailor advertisements.

H.2 Data ownership

The following items should be considered:

a) check whether the service provider reserves rights to use, disclose, or make public your information;

b) check whether the IP rights of the data you own remain intact;

c) check whether the service provider retains rights to your information even if you remove your data from the cloud;

d) understand whether you can move or transfer your data and the service to another provider when you want to, and whether export utilities are available and are easy to use; and

e) check whether data can be permanently erased from the cloud, including any backup storage, when you delete this data or when you end the service.

H.3 Additional selection considerations

The following items should be considered:

a) understand the acceptable range of risks associated with the use of cloud services;

b) select a service provider with a service level agreement commensurable with the importance of your business function;

c) select a service provider that can explain clearly what security features are available, preferably supported by an independent information security management certification (e.g., ISO/IEC 27001);

d) select a service provider with no major security incident reported, or one that can provide transparency to previous security incidents with cause and remediation explained;

e) select a service provider that ensures data confidentiality by complying to the following:

   i) using encryption (e.g. Secure Sockets Layer (SSL)) to transmit data; and

   ii) using encryption to protect stored static data. (If not, you have to use your own encryption before storing data in the cloud. In that case, remember to keep your encryption key safe.)

f) select a service provider that provides a simple and clear reporting mechanism for service problems, security and privacy incidents;

g) select a service provider that provides regular service management reports and incident problem reports;

h) ask for samples of data that will be returned upon the termination of service and ensure that they are readable and can be recovered when needed; and

j) check for interoperability between the cloud service and external systems and select a service provider that can meet your requirements in terms of:

   i) the ability for other authorised sites or systems (e.g., your internal systems) to use the data or system functions that have been hosted under the cloud service, with standard-based and well-documented programming interfaces;

   ii) the ability to access and work with data or functions provided at some other sites that are not managed by the cloud service provider;

   iii) the ability to track for updates that are made on other sites, and automatically keep the corresponding data up to date under the cloud service; and

   iv) the ability to notify another system on the updates made under the cloud service, or provide a way for others to ask for the updates made.

Bibliography

[1] ISO 22301, *Security and resilience - Business continuity management systems - Requirements*

[2] ISO 31000, *Risk Management*

[3] ISO/IEC 19086-1, *Information technology - Cloud computing - Service Level Agreement (SLA) framework - Part 1: Overview and concepts*

[4] ISO/IEC 27036-4, *Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services*

[5] ITU-T X.1601, *Cloud computing security - Overview of cloud computing security*

[6] CREST, *Cyber Security Incident Response Supplier Selection Guide*

[7] ENISA, *Cloud Standards and Security*

[8] Cloud Security Alliance, *Cloud Controls Matrix*

[9] Cloud Security Alliance, *Top Threats to Cloud Computing V1.0.*

[10] Payment Card Industry (PCI) Data Security Standard, *Requirements and Security Assessment Procedures*

[11] CyberSecurity Malaysia, *Guidelines for Securing Cloud Implementation by Cloud Service Subscriber*

[12] IBM, Cloud Computing Use Cases Whitepaper Version 4.0, *Review and summary of cloud service level agreements*

[13] Cloud industry forum, *8 criteria to ensure you select the right cloud service provider*
https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider

[14] Developing a Cloud Provider Selection Model
https://subs.emis.de/LNI/Proceedings/Proceedings190/163.pdf

[15] Info Cloud, *Checklist for SMEs on selecting Cloud Service Provider*
http://www.infocloud.gov.hk/home/10785

Acknowledgements

Members of the Application Security Sub Working Group

Mr Azlan Mohamed Ghazali (Chairman)	KPMG Management and Risk Consulting Sdn. Bhd.
Mr Mohd Fairuz Ismail (Vice Chairman)	KPMG Management and Risk Consulting Sdn. Bhd.
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Dr Dzaharudin Mansor / Ms Mira Ajib	American Malaysian Chamber of Commerce
Mr Fam Jun Xiang	Celcom Axiata Berhad
Mr Mohd Nazaruddin Shamsudin	Digi Telecommunications Sdn Bhd
Mr Russell - Md Ifthekharul Alam	Maxis Broadband Sdn Bhd
Ms Patrina Nasiron/ Mr Thaib Mustafa	Telekom Malaysia Berhad

By invitation:

Ms Lin En Shu	Alibaba Cloud
Mr Fadli Che Yusoff	Amazon Web Services (AWS)
Ms Norahana Salimin	CyberSecurity Malaysia
Ms Azleyna Ariffin/ Mr Harme Mohamed/ Ms Siti Hajar Roslan	National Cyber Security Agency