MCMC MTSFB TC G017:XXXX

TECHNICAL CODE

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

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

MCMC MTSFB TC G017:XXXX

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 which supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) consists of representatives from the following organisations:

Alibaba Cloud

Amazon Web Services (AWS)

American Malaysian Chamber of Commerce

Celcom Axiata Berhad

CyberSecurity Malaysia

Digi Telecommunications Sdn Bhd

KPMG Management and Risk Consulting Sdn. Bhd.

Maxis Broadband Sdn Bhd

Persatuan Industri Komputer dan Multimedia Malaysia

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.

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

e) moved sub-clause 7.5, *Exit provisions* to Annex G; and

f) added and modified checklist of risk mitigation controls in Annex E.

This Technical Code cancels and replaces the MCMC MTSFB TC G018:2018, *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 depends on the services offering. In general cloud services provide an advantage such on 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 on 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 Cloud Service Users (CSU) 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 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 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 any 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*

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 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.

4.2 Cloud service customer

Organisation or party which is in a business relationship for the purpose of using cloud services.

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

4.3 Cloud Service Partner (CSP)

Cloud Service Partner (CSP) is a party which engage in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

4.4 Cloud service provider

Party which makes cloud services available.

4.5 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.

4.6 End points

Refers to any devices that being used to connect to the cloud services such as Personal Computers (PCs), mobile, Internet of Things (IoT) devices and etc.

4.7 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

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:

a) IaaS;

b) Platform as a Service (PaaS); and

c) SaaS.

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

5.1 Cloud Service Subscribers (CSS) and Cloud Service Provider (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.

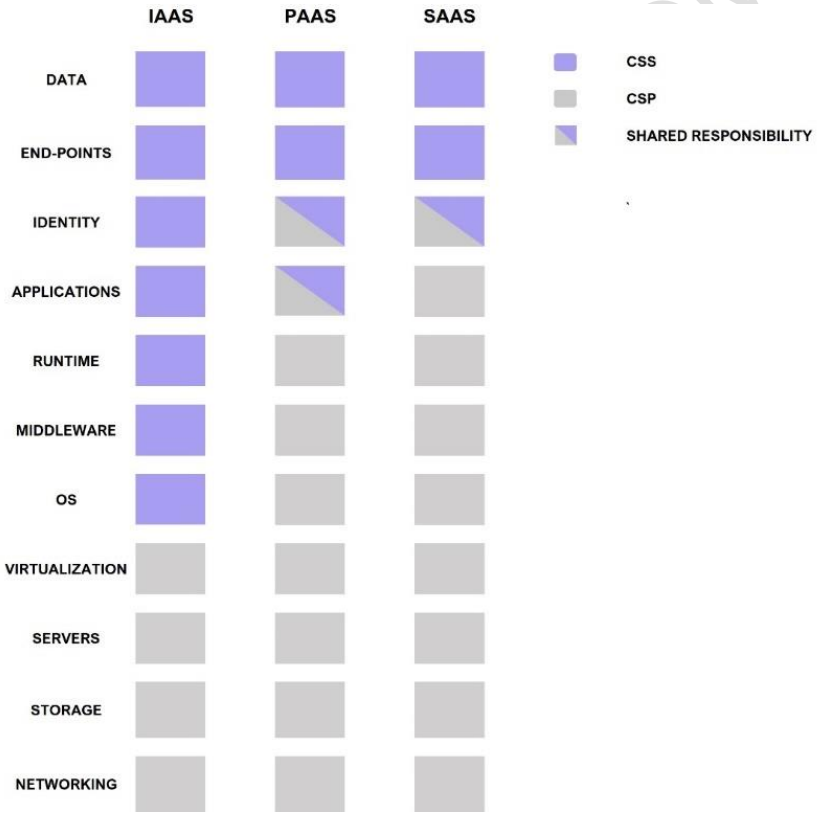

Figure 1. CSP and CSS responsibilities on cloud service models

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 to 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 in 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 are shift more to the CSP compare to the CSS. The CSS is still responsible on managing the data and endpoints while the responsibility of applications and identify is appropriately shared.

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

6. Risk assessment

While the benefits of adopting cloud computing offers 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 foregoing the business advantages using cloud, or using cloud in a way that 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, *Information and Network Security - Requirements*.

The following sections expands 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.

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) cybersecurity team;

d) risk management team; and

e) legal.

6.2 Scope, context and criteria

The scope of the cloud-based IT solution that in turn will 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 being developed, 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) criterial 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 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 E) could be included to reduce the impact and/or likelihood.

c) Evaluate risk

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

   ii) The CSP successfully justify 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 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 should be based on the CSP which best meet CSS risk tolerance specified during the risk management process (refer Clause 6).

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

ii) CSP selected may 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 and etc.

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

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

i) Payment Card Industry Data Security Standard (PCIDSS);

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

iii) for Business Continuity Management (BCM) and resiliency: ISO 22301 or equivalent

NOTE: Refer Annex D for example of cloud control matrix.

c) CSP selected should 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 are transparent with partnership and outsourcing to the third parties.

7.2.1 Cloud Service Provider (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 irregardless of their dependency on subcontractors; and

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

7.2.2 CMI Industry Partners

Partners of CMI industries such as content providers and resellers that are small enterprises should leverage on compliant CSP services to deliver their product and services. Their responsibility as a CSS (shown in Figure 1) should be governed by the following instead:

a) contractual obligations with CMI; and

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

Above requirements is to support local innovation opportunities for small enterprises in CMI industries,

7.3 Contracts, commercials and Service Level Agreements (SLAs)

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

The organisations shall conduct due diligence 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 varies depend on the subscribed services such IaaS, PaaS or SaaS.

The organisations shall aware all the associated risk and threat prior 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 employee screening process.

CSP employees sharing administrator passwords, or otherwise leaving credentials unsecure (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 unauthorised user, which can occur from both outside the organisation and within the organisation. Data breach from organisation can have a huge impact on its business regarding finance, trust and loss of customers. This may happen accidently due to flaws in infrastructure, application designing, operational issues, insufficiency of authentication, authorisation, and audit controls.

A.4 Data loss

Data loss is a sensitive matter for any 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 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 is 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 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.

A.9 Account or service hijacking

Account hijacking involves the stealing of user credentials to get an access 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 including phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow 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.

A.11 Malicious intent

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

Annex B
(informative)

Abbreviations

AES	Advanced Encryption Standard
API	Applications and Programming Interface
ARP	Address Resolution Protocol
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
CMI	Communications and Multimedia Industry
CPU	Central Processing Unit
CSA CCM	Cloud Security Alliance Cloud Controls Matrix
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSS	Cloud Service Subscribers
CSU	Cloud Service User
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster Recovery
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IoT	Internet of Things
IP	Intellectual Property
ISMP	Information Security Management Program
ISMS	Information Security Management System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
MAC	Media Access Control
OS	Operating System
OWASP	Open Web Application Security Project
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
SLA	Service Level Agreement
SLO	Service Level Objective
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
SSO	Single Sign-On
TLS	Transport Layer Security
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.

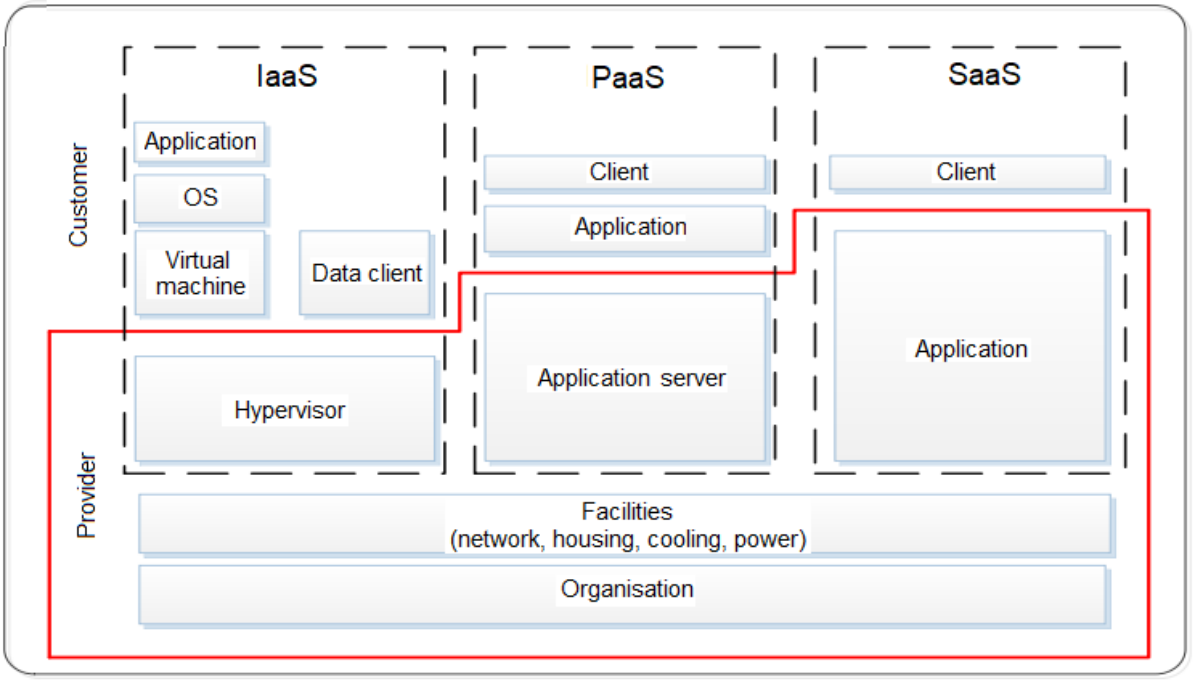

Figure C.1. Map of different technologies in the different types of cloud services

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

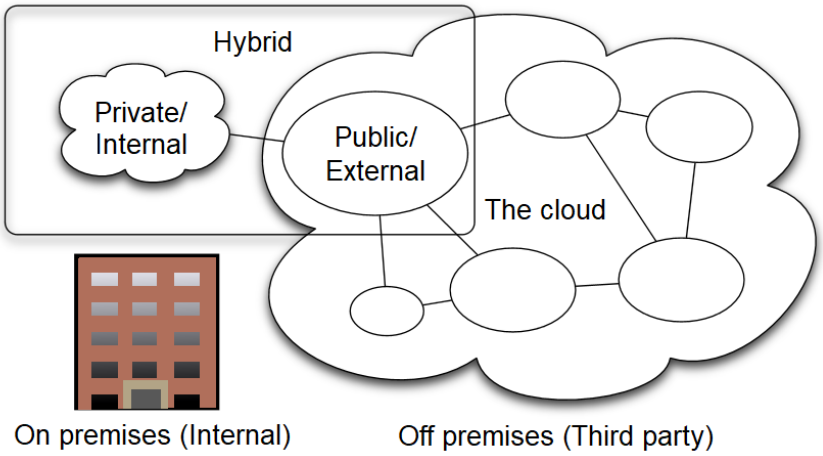

Figure C.2. Cloud computing types

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
Account type	Single tenant	Multi-tenant	Combination or tenants. Private or Public cloud.	A multi-tenant platform that is accessible only for a specific subset of customer
Premises type	Owned premises and managed by the organisation	Owned and managed by the service provider. Off-premises / Third Party	Owned and managed by multiple organisation	Owned and managed by multiple organisation
Data management type	Data management policy is self-managed by the organisation.	Data management policy is bound to multi-tenant data policy.	Each organisation manages data management policy.	Data management policy is managed by each organisation.
Security management	High level of data security	Security dependent on CSP	Security depending on CSP and CSS	Security depending managed by each organisation and CSS
Risk management	Low level of risk	Risk dependent on CSP	Medium level of risk	Risk dependent on each organisation

Annex D
(informative)

Cloud controls matrix

Table D.1. Cloud controls matrix for application and interface security

Control domain	CCM V3.0 Control ID	Updated control specification
Application security	AIS-01	APIs shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. Open Web Application Security Project (OWASP)) for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
Customer access requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.
Data integrity	AIS-03	Data input and output integrity routines (i.e. reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data or misuse.
Data security/integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration or destruction.

Table D.2. Cloud controls matrix for audit assurance and compliance

Control domain	CCM V3.0 Control ID	Updated control specification
Audit planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities shall be agreed upon prior to executing any audits.
Independent audits	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organisation addresses nonconformities of established policies, standards, procedures and compliance obligations.
Information system regulatory mapping	AAC-03	Organisations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.

Table D.3. Cloud controls matrix for BCM and operational resilience

Control domain	CCM V3.0 Control ID	Updated control specification
Business continuity planning	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance and information security requirements.
Business continuity planning	BCR-01	Requirements for business continuity plans include the following: a) defined purpose and scope, aligned with relevant dependencies; b) accessible to and understood by those who will use them; c) owned by a named person(s) who is responsible for their review, update and approval; d) defined lines of communication, roles and responsibilities; e) detailed recovery procedures, manual work-around and reference information; and f) method for plan invocation.
Business continuity testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organisational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.
Data centre utilities/environmental conditions	BCR-03	Data centre utilities services and environmental conditions (e.g. water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorised interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.
Documentation	BCR-04	Information system documentation (e.g. administrator and user guides, and architecture diagrams) shall be made available to authorised personnel to ensure the following: a) configuring, installing, and operating the information system; and b) effectively using the system's security features.
Environmental risks	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.
Equipment location	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorised access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.
Equipment maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.
Equipment power failures	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.

Table D.3. Cloud controls matrix for BCM and operational resilience *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
Impact analysis	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organisation (cloud provider, cloud consumer) that shall incorporate the following: a) Identify critical products and services. b) Identify all dependencies, including processes, applications, business partners, and third-party service providers. c) Understand threats to critical products and services. d) Determine impacts resulting from planned or unplanned disruptions and how these vary over time. e) Establish the maximum tolerable period for disruption. f) Establish priorities for recovery. g) Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption. h) Estimate the resources required for resumption.
Policy	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organisation's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., Information Technology Infrastructure Library (ITIL) v4 and Control Objectives for Information and Related Technology (COBIT) 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.
Retention policy	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.

Table D.4. Cloud controls matrix for change control and configuration management

Control domain	CCM V3.0 Control ID	Updated control specification
New development/ acquisition	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data centre facilities have been pre-authorised by the organisation's business leadership or other accountable business role or function.
Outsourced development	CCC-02	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organisation (e.g. ITIL service management processes).
Quality testing	CCC-03	Organisations shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.
Unauthorised software installations	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorised software on organisationally-owned or managed user end-point devices (e.g. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
Production changes	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: a) Business-critical or customer (tenant)-impacting (physical and virtual) applications and API designs and configurations. b) Infrastructure network and systems components.
Production changes	CCC-05	Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorisation by, the customer (tenant) as per agreement (SLA) prior to deployment.

Table D.5. Cloud controls matrix for data security and information lifecycle management

Control domain	CCM V3.0 Control ID	Updated control specification
Classification	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity and criticality to the organisation.
Data inventory/flows	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.
Ecommerce transactions	DSI-03	Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorised disclosure, or modification in such a manner to prevent contract dispute and compromise of data.
Handling/labelling/ security policy	DSI-04	Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
Non-production data	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and shall comply with all legal and regulatory requirements for scrubbing of sensitive data elements.
Ownership/ stewardship	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.
Secure disposal	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

Table D.6. Cloud controls matrix for data centre security

Control domain	CCM V3.0 Control ID	Updated control specification
Asset management	DCS-01	Assets shall be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly and assigned ownership by defined roles and responsibilities.
Controlled access points	DCS-02	Physical security perimeters (e.g. fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.
Equipment identification	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.
Off-site authorisation	DCS-04	Authorisation shall be obtained prior to relocation or transfer of hardware, software, or data to an off-site premise.
Off-site equipment	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organisation's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.
Policy	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas storing sensitive information.
Secure area authorisation	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorised personnel are allowed access.
Unauthorised persons entry	DCS-08	Ingress and egress points such as service areas and other points where unauthorised personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorised data corruption, compromise, and loss.
User access	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.

Table D.7. Cloud controls matrix for encryption and key management

Control domain	CCM V3.0 Control ID	Updated control specification
Entitlement	EKM-01	Keys shall have identifiable owners (binding keys to identities) and there shall be key management policies.
Key generation	EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g. lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.
Sensitive data protection	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g. file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g. system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
Storage and access	EKM-04	Platform and data-appropriate encryption (e.g. Advanced Encryption Standard (AES-256)) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question) but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.

Table D.8. Cloud controls matrix for governance and risk management

Control domain	CCM V3.0 Control ID	Updated control specification
Baseline requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organisationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations shall be authorised following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements shall be reassessed at least annually unless an alternate frequency has been established and authorised based on business needs.
Data focus risk assessments	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: a) awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure; b) compliance with defined retention periods and end-of-life disposal requirements; and c) data classification and protection from unauthorised use, access, loss, destruction, and falsification.
Management oversight	GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.
Management program	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorised access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: a) risk management; b) security policy; c) organisation of information security; d) asset management; e) human resources security; f) physical and environmental security; g) communications and operations management; h) access control; and information systems acquisition, development, and maintenance.
Management support/involvement	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment and shall ensure the action has been assigned.
Policy	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies shall be authorised by the organisation's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.

Table D.8. Cloud controls matrix for governance and risk management *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
Policy enforcement	GRM-07+B30	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures shall be stated in the policies and procedures.
Policy impact on risk assessments	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.
Policy reviews	GRM-09	The organisation's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organisation to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.
Risk assessments	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g. audit results, threat and vulnerability analysis, and regulatory compliance).
Risk management framework	GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.

Table D.9. Cloud controls matrix for human resources

Control domain	CCM V3.0 Control ID	Updated control specification
Asset returns	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organisationally-owned assets shall be returned within an established period.
Background screening	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.
Employment agreements	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and shall be signed by newly hired or on-boarded workforce personnel (e.g. full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.
Employment termination	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.
Mobile device management	HRS-05	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g. mandated security training, stronger identity, entitlement and access controls, and device monitoring).
Non-disclosure agreements	HRS-06	Requirements for non-disclosure or confidentiality agreements reflecting the organisation's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.
Roles/responsibilities	HRS-07	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.
Technology acceptable use	HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organisationally-owned or managed user end-point devices (e.g. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., Bring Your Own Device (BYOD)) shall be considered and incorporated as appropriate.
Training/awareness	HRS-09	A security awareness training program shall be established for all contractors, third party users, and employees of the organisation and mandated when appropriate. All individuals with access to organisational data shall receive appropriate awareness training and regular updates in organisational procedures, processes, and policies relating to their professional function relative to the organisation.
User responsibility	HRS-10	All personnel shall be made aware of their roles and responsibilities for: a) maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations; and b) maintaining a safe and secure working environment.

Table D.9. Cloud controls matrix for human resources *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
Workspace	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g. on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.

Table D.10. Cloud controls matrix for identity and access management

Control domain	CCM V3.0 Control ID	Updated control specification
Audit tools access	IAM-01	Access to, and use of, audit tools that interact with the organisation's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.
Credential lifecycle/provision management	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organisationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures shall incorporate the following: a) Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g. internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships). b) Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g. management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically distributed deployments, and personnel redundancy for critical systems). c) Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g. provider and/or other customer (tenant)). d) Identity trust verification and service-to-service API and information processing interoperability (e.g. Single Sign-On (SSO) and federation). e) Account credential lifecycle management from instantiation through revocation. f) Account credential and/or identity store minimisation or re-use when feasible. g) Authentication, authorisation, and accounting AAA rules for access to data and sessions (e.g. encryption and strong/multi-factor, expirable, non-shared authentication secrets). h) Permissions and supporting capabilities for customer (tenant) controls over AAA rules for access to data and sessions. i) Adherence to applicable legal, statutory, or regulatory compliance requirements.
Diagnostic/configuration ports access	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorised individuals and applications.

Table D.10. Cloud controls matrix for identity and access management *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
Policies and procedures	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.
Segregation of duties	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.
Source code access restriction	IAM-06	Access to the organisation's own developed applications, program, or object source code, or any other form of Intellectual Property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.
Third party access	IAM-07	The identification, assessment, and prioritisation of risks posed by business processes requiring third party access to the organisation's information systems and data shall be followed by coordinated application of resources to minimise, monitor, and measure likelihood and impact of unauthorised or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.
Trusted sources	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.
User access authorisation	IAM-09	Provisioning user access (e.g. employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organisationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorised by the organisation's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.
User access reviews	IAM-10	User access shall be authorised and revalidated for entitlement appropriateness, at planned intervals, by the organisation's business leadership or other accountable business role or function supported by evidence to demonstrate the organisation is adhering to the rule of least privilege based on job function. For identified access violations, remediation shall follow established user access policies and procedures.
User access revocation	IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organisationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g. termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.

Table D.10. Cloud controls matrix for identity and access management *(concluded)*

Control domain	CCM V3.0 Control ID	Updated control specification
User ID credentials	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: a) identity trust verification and service-to-service application (API) and information processing interoperability (e.g. SSO and federation); b) account credential lifecycle management from instantiation through revocation; c) account credential and/or identity store minimisation or re-use when feasible; and d) Adherence to industry acceptable and/or regulatory AAA rules (e.g. strong/multi-factor, expirable, non-shared authentication secrets)
Utility programs access	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.

Table D.11. Cloud controls matrix for infrastructure and virtualisation security

Control domain	CCM V3.0 Control ID	Updated control specification
Audit logging/intrusion detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviours and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.
Change detection	IVS-02+B82	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images shall be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity shall be immediately available to customers through electronic methods (e.g. portals or alerts).
Clock synchronisation	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronise the system clocks of all relevant information-processing systems to facilitate tracing and reconstitution of activity timelines.
Information system documentation	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.
Vulnerability management	IVS-05+B84	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualisation technologies used (e.g. virtualisation aware).
Network security	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.

Table D.11. Cloud controls matrix for infrastructure and virtualisation security *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
OS hardening and base controls	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.
Production/ Non-production environments	IVS-08	Production and non-production environments shall be separated to prevent unauthorised access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.
Segmentation	IVS-09	Multi-tenant organisationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: a) Established policies and procedures. b) Isolation of business-critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance. c) Compliance with legal, statutory, and regulatory compliance obligations.
Virtual Machine (VM) Security - data protection	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualised servers and, where possible, shall use a network segregated from production-level networks for such migrations.
Hypervisor hardening	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualised systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, internet protocol address filtering, firewalls, and Transport Layer Security (TLS) encapsulated communications to the administrative consoles).
Wireless security	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: a) Perimeter firewalls implemented and configured to restrict unauthorised traffic. b) Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g. encryption keys, passwords, and Simple Network Management Protocol (SNMP) community strings). c) User access to wireless network devices restricted to authorised personnel. d) The capability to detect the presence of unauthorised (rogue) wireless network devices for a timely disconnect from the network.

Table D.11. Cloud controls matrix for infrastructure and virtualisation security *(concluded)*

Control domain	CCM V3.0 Control ID	Updated control specification
Network architecture	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g. deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g. Media Access Control (MAC) spoofing and Address Resolution Protocol (ARP) poisoning attacks) and/or Distributed Denial-of-Service (DDoS) attacks.

Table D.12. Cloud controls matrix for interoperability and portability

Control domain	CCM V3.0 Control ID	Updated control specification
APIs	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.
Data request	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g. .doc, .xls, .pdf, logs, and flat files).
Policy and legal	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service API and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.
Standardised network protocols	IPY-04	The provider shall use secure (e.g. non-clear text and authenticated) standardised network protocols for the import and export of data and to manage the service and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
Virtualisation	IPY-05	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 and all solution-specific virtualisation hooks available for customer review.

Table D.13. Cloud controls matrix for mobile security

Control domain	CCM V3.0 Control ID	Updated control specification
Anti-malware	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.
Application stores	MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.
Approved applications	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.
Approved software for Bring Your Own Device (BYOD)	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.
Awareness and Training	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.
Cloud based services	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.
Compatibility	MOS-07+B105	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.
Device eligibility	MOS-08+B106	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.
Device inventory	MOS-09+B107	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.
Device management	MOS-10	A centralised, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.
Encryption	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.
Jailbreaking and rooting	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralised device management system (e.g. mobile device management).
Legal	MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.
Lockout screen	MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.
OS	MOS-15	Changes to mobile device OS, patch levels, and/or applications shall be managed through the company's change management processes.

Table D.13. Cloud controls matrix for mobile security *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
Passwords	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.
Policy	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).
Remote wipe	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.
Security patches	MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorised IT personnel shall be able to perform these updates remotely.
Users	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.

Table D.14. Cloud controls matrix for security incident management, e-discovery and cloud forensics

Control domain	CCM V3.0 Control ID	Updated control specification
Contact/authority maintenance	SEF-01+B119	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g. change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.
Incident management	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.
Incident reporting	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.
Incident response legal preparation	SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.
Incident response metrics	SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.

Table D.15. Cloud controls matrix for supply chain management, transparency and accountability

Control domain	CCM V3.0 Control ID	Updated control specification
Data quality and integrity	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.
Incident reporting	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).
Network/infrastructure services	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.
Provider internal assessments	STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.
Supply chain agreements	STA-05	Supply chain agreements (e.g. SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: a) Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations). b) Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships. c) Notification and/or pre-authorisation of any changes controlled by the provider with customer (tenant) impacts. d) Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain). e) Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organisation being assessed. f) Expiration of the business relationship and treatment of customer (tenant) data impacted. g) Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence.

Table D.15. Cloud controls matrix for supply chain management, transparency and accountability *(continued)*

Control domain	CCM V3.0 Control ID	Updated control specification
Supply chain governance reviews	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.
Supply chain metrics	STA-07+B130	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g. SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.
Third party assessment	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.
Third party audits	STA-09+B132	Third party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third party contracts. Third party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.

Table D.16. Cloud controls matrix for threat and vulnerability management

Control domain	CCM V3.0 Control ID	Updated control specification
Anti-virus/malicious software	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organisationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
Vulnerability/patch management	TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organisationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritising remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organisation's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.
Mobile code	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorised mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organisationally-owned or managed user end-point devices (e.g. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.

Annex E
(informative)

Recommended risk mitigation (controls) checklist

Table E.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 E.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 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 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 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 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 somethings 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 to 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 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 better still 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. Terms for 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 customer and provider.	a) Agree on scope of work, roles and responsibilities of the service and deliverables and how that is distributed between customer and provider; b) confirm on 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 Business Continuity Plan (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 for agreement *(continued)*

No	Main terms	Contents	Descriptions
4.	Legal protections	Specific terms relating to indemnification, IP rights, limitation of liability and warranties.	a) Know the specific clause relating to indemnification, IP rights, limitation of liability and warranties 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.	b) The scope of services the CSP will deliver and a complete definition of each service; c) service delivery Metrics and auditing mechanism; d) responsibilities of both parties and remedies available to both if the terms of the SLA are not met; and e) 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 on 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	ISO/IEC 19086-4	

G.2 Cloud Service Provider (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 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 possessed 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 on the system response speed;

b) reliability to measure system availability;

c) system availability;

d) latency;

e) load balance;

f) durability to measure on how likely to lose data;

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

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

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

j) automation to measure on 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 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 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 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 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 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, *Top Threats to Cloud Computing V1.0.*

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

[10] 8 criteria to ensure you select the right cloud service provider | Cloud industry forum https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider

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

[12] Tips for Small and Medium Enterprises in Choosing Cloud Service Providers http://www.infocloud.gov.hk/home/10785

[13] Developer Works Cloud Computing Editors IBM. (2010). Review and Summary of Cloud Service Level Agreements. Retrieved on 14 January 2013, from http://agimo.govspace.gov.au/files/2011/11/Cloud-Legal-Draft-Better-Practice-Guide-November-2011.pdf
http://www.ibm.com/developerworks/cloud/library/cl-rev2sla-pdf.pdf

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
Ms Lin En Shu	Alibaba Cloud
Mr Fadli Che Yusoff	Amazon Web Services (AWS)
Ms Mira Ajib	American Malaysian Chamber of Commerce
Mr Fam Jun Xiang	Celcom Axiata Berhad
Ms Norahana Salimin	CyberSecurity Malaysia
Mr Mohd Nazaruddin Shamsudin	Digi Telecommunications Sdn Bhd
Mr Russell - Md Ifthekharul Alam	Maxis Broadband Sdn Bhd
Ms Azleyna Ariffin/ Mr Harme Mohamed/ Ms Siti Hajar Roslan	National Cyber Security Agency
Dr Dzaharudin Mansor	Persatuan Industri Komputer dan Multimedia Malaysia
Ms Patrina Nasiron	Telekom Malaysia Berhad

MALAYSIAN TECHNICAL STANDARDS FORUM BHD

MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia, Jalan Impact
63000 Cyberjaya,
Selangor Darul Ehsan

Tel: (+603) 8320 0300
Fax: (+603) 8322 0115
Website: www.mtsfb.org.my