INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS) Implementation Guideline Report

For cross-certification from ISO/IEC 27001:2005 to MTCS SS

December 2014

Revision History

Revision Date	Version	Updated by	Description
February 2014	Version 1.0	IDA	Initial release
December 2014	Version 1.1	IDA	Corrective or editorial revisions

Disclaimer

The information provided in this Implementation Guideline Report is for general information purposes only. The Implementation Guideline Report is provided "AS IS" without any express or implied warranty of any kind. Whilst the Working Group (defined below), Infocomm Development Authority of Singapore (IDA) and / or individual contributors thereof have made every reasonable effort to ensure that the information contained herein are obtained from reliable sources and that any opinions and / or conclusions drawn there from are made in good faith, to the extent not prohibited by law, the Working Group and IDA, and their respective employees, agents and / or assigns shall not be responsible or liable for reliance by any person on the information, opinions and / or conclusions contained herein. The Working Group and IDA, and their respective employees, agents and / or assigns shall not be liable for any direct, indirect, incidental or consequential losses arising out of the use of the Implementation Guideline Report. The Working Group and IDA are entitled to add, delete or change any information in the Implementation Guideline Report at any time at their absolute discretion without giving any reasons.

The Multi-tiered Cloud Security cross-certification Working Group was appointed by Infocomm Development Authority (IDA) to assist in the preparation of this report. It comprises the following experts who contribute in their individual capacity:

		Name
Facilitator	:	Tao Yao Sing
Secretary		Aaron Thor
Members		Lam Kwok Yan
		Wong Onn Chee
		Alan Sinclair
		Gregory Malewski (alternate to Alan Sinclair)
		John Yong
		Hector Goh (alternate to John Yong)

The experts of the Working Group are affiliated with:

- Infocomm Development Authority of Singapore
- MOH Holdings Pte Ltd
- PrivyLink Pte Ltd
- Resolvo Systems Pte Ltd

The Multi-Tiered Cloud Security cross-certification Focus Group on ISO/IEC 27001:2005 to MTCS SS was appointed by IDA to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

Jason Kong	BSI Group Singapore Pte Ltd
Cheng Loon, Dave	Certification International (Singapore) Pte Ltd
Ros Oh	DNV Business Assurance Singapore Pte Ltd
Lee Lai Mei	SGS International Certification Services Singapore Pte Ltd
Indranil Mukherjee	Singapore ISC Pte Ltd
Carol Sim	TÜV Rheinland Singapore Pte Ltd
Chris Ng	TÜV SÜD PSB Pte Ltd

Please send questions and feedback to IDA_cloud@ida.gov.sg.

Contents

1 Normative References

The following source documents were referenced for the purpose of this Report:

- **Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS).** MTCS SS aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS SS provides relevant cloud computing security practices and controls for cloud users, Auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers to strengthen and demonstrate the cloud security controls in their cloud environments.

- **ISO/IEC 27001:2005** *Information technology -- Security techniques -- Information security management system requirements*. ISO/IEC 27001 is the international standard for information security management which defines a set of controls and requirements to establish, implement, operate, monitor, review, maintain and improve an information security management system (ISMS). ISO/IEC 27001:2005 benefits entities in allowing them to demonstrate commitment and compliance via the adoption of this standard.

Documents which provide additional context, including examples and guidance which may or may not have been implemented by the Cloud Service Providers, such as ISO/IEC 27002, are not covered in this report.

2 Purpose of Document

This Implementation Guideline Report is the second report in the set of three (3) documents to support cross-certification between ISO/IEC 27001:2005 and MTCS SS. The purpose of each document is described in the diagram below.

Gap Analysis Report	Implementation Guideline Report	Audit Checklist Report
The purpose of the Gap Analysis Report is to provide an overview of the differences between the requirements listed in MTCS SS and ISO/IEC 27001:2005 Standard. The information provided in this document aims to assist entities that are ISO/IEC 27001:2005 certified to adopt the MTCS SS. Cloud Service Providers that are ISO/IEC 27001:2005 certified will have to comply with the requirements stated in MTCS SS that are currently omitted in ISO/IEC 27001:2005.	The purpose of the Implementation Guideline Report is meant to assist Cloud Service Providers that are ISO/IEC 27001:2005 certified to implement MTCS SS. The guidelines in the report are generic and need to be tailored to each Cloud Service Provider's specific requirements.	The purpose of the Audit Checklist Report is to guide Auditors including internal audit function, MTCS SS Certification Bodies and external audit bodies in understanding additional requirements beyond ISO/IEC 27001:2005. From the Cloud Service Providers' perspective, this document serves as a general guide for these providers to understand the scope covered in MTCS SS certification audit when the scope of ISO/IEC 27001:2005 audit overlaps with scope of MTCS SS audit.

3 Intended Audience

This Implementation Guideline Report is intended for Cloud Service Providers that are ISO/IEC 27001:2005 certified and interested in obtaining MTCS SS Levels 1, 2 or 3.

This report is also intended to guide Auditors, including internal audit function, MTCS SS Certification Bodies and external audit bodies on the differences between MTCS SS and ISO/IEC 27001:2005, and the corresponding implementation guideline.

4 Document Structure

This document has the following structure from this section onwards. Sections 6, 7 and 8 have introduction statements that will explain the section's background and context in more details.

- Section 5 – Terms and Definitions
- Section 6 – Scope
- Section 7 – Tips on Using this Implementation Guideline Report
- Section 8 – Implementation Guidelines

5 Terms and Definitions

ISMS-related terms used in this report are defined in ISO/IEC 27001:2005, and cloud-related terms used in this report are defined in MTCS SS.

6 Scope

In order to assist Cloud Service Providers that are ISO/IEC 27001:2005 certified to adopt the MTCS SS, we have developed this Implementation Guideline Report for the gaps identified in Gap Analysis Report, which are classified as “INCREMENTAL” or “NEW”.

For ease of reference, the description of the gap classifications is listed below. For the full report on the gap analysis, refer to the Gap Analysis Report.

Gap Classification	Description
INCREMENTAL	Indicates the clauses in MTCS SS that are stated with more details than the corresponding sections in clauses in ISO/IEC 27001:2005. In general, the requirements are classified as "INCREMENTAL" if the required enhancements on the existing ISO/IEC 27001:2005 characteristics are not costly or onerous in nature.
NEW	Indicates the clauses in MTCS SS that are absent, or stated with significantly more details than the corresponding sections and clauses in ISO/IEC 27001:2005. In general, the requirements are classified as "NEW" if there may be a material financial cost to meet the relevant MTCS SS requirement, additional controls to be included in the audit checklist and / or the effort is relatively onerous.

Note that requirements that were listed as “INCLUDED” in the Gap Analysis Report will not be discussed in this document.

Gap Classification	Description
INCLUDED	Indicates the number of clauses in MTCS SS that are equally represented in ISO/IEC 27001:2005.

7 Tips on Using this Implementation Guideline Report

This document is meant to help Cloud Service Providers who are ISO/IEC 27001:2005 certified and are implementing or planning to implement the MTCS SS Levels 1, 2 or 3. The guidelines are generic and service providers will need to tailor the suggested guidelines to their specific requirements.

Cloud Service Providers should refer to the implementation guidelines listed for the targeted and preceding Level if they are looking to be certified in MTCS SS Levels 2 or 3. For example, if a Cloud Service Provider is looking to be certified in MTCS SS Level 3, the provider should refer to implementation guideline listed in Section 8.3 ‘MTCS SS Level 3’, as well as the preceding Levels, Section 8.1 ‘ MTCS SS Level 1’ and Section 8.2 ‘MTCS SS Level 2’.

While there may be multiple instances of certain activities (e.g., training, reviews) in various sections of the MTCS SS, Cloud Service Providers may opt to combine such activities into a single activity with a scope covering the relevant areas in order to optimise resources or improve efficiency.

For example, training activities are mentioned in MTCS SS Clauses 7.6 'Information security training and awareness', 10.3 'Prevention of misuse of cloud facilities' and 11.2 'Information security incident response plan testing and updates'. As such, Cloud Service Providers can choose to structure their training session in a single session, or across multiple sessions.

Similarly, reviews and/or audits are mentioned in MTCS SS Clauses 6.5 'Review of information security policy', 6.6 'Information security audits', 13.0 'Audit logging and monitoring' and 18.6 'Physical security review'. The Cloud Service Providers can choose to structure their reviews and / or audits in a single exercise or across multiple reviews and / or audits as per organisation's preference.

MTCS SS has several requirements that are mutually exclusive across MTCS SS Levels 1, 2 and 3. Cloud service providers should note that they can only comply with requirements for the specific level in areas involving frequency of activities. For example, in MTCS SS Clause 15.1 'Vulnerability scanning', Cloud Server Providers have to conduct vulnerability scanning more frequently as they are looking to be certified in the next level.

Where "all" and "most" are mentioned and no additional detailed description is included within this Implementation Guideline Report, Cloud Service Providers are encouraged to refer to the MTCS SS to further understand the context and scope covered for the specific requirement.

8 Implementation Guidelines

8.1 MTCS SS Level 1

This section summarises the implementation guidelines for gaps identified between MTCS SS Level 1 and ISO/IEC 27001:2005.

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
6	**Information security management**	
6.1	**Information security management system (ISMS)**	
6.1.2(e) Incremental	ISO/IEC 27001:2005 does not cover risk mitigation specific to authorised insiders. The Cloud Service Provider shall implement controls to mitigate risks from authorised insiders (including internal and third parties) by considering the following measures: • Scope of risk mitigation to cover security policies and procedures, security infrastructure design and implementation, approval structure for operations, user access matrix, audit trail and usage logs, and tenancy and customer isolation procedures (including virtualisation) • Consider implementing an identity management system to coordinate authentication and authorisation, including some form of password management control such as different user access profiles for different areas of the system, and clear access approval structure for specific areas. Refer to MTCS SS Clause 22.0 for additional details	Controls to mitigate risks mentioned in general but not specific for authorised insiders.
6.1.2(i) Incremental	ISO/IEC 27001:2005 does not cover risk mitigation specific to cloud computing. The Cloud Service Provider shall implement controls to mitigate risks associated with cloud computing in policies and procedures. Cloud Service Providers shall include both traditional risk categories and cloud specific risks covering the areas of governance, infrastructure, operations management, services, user access, tenancy, customer isolation, and virtualisation. It is critical to identify cloud specific risks in the areas as listed above and incorporate the mitigation steps in the policies and procedures. As a reference, see TR30:2012 Technical Reference for Virtualisation Security for servers Annex A for a risk assessment worksheet on security in virtualisation.	Controls to mitigate risks mentioned in general but not specific for cloud computing.

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
6.1.2(j) Incremental	ISO/IEC 27001:2005 does not cover security controls specific to virtualisation. The Cloud Service Provider shall implement controls related to virtualisation security for cloud services in policies and procedures including, but not limited to the list of areas as listed in MTCS SS Clause 6.1.2(j). See TR 30:2012 Technical Reference for Virtualisation Security for servers for additional details.	No mention of "virtualisation", although generic security controls are mentioned. Additional security measures required for virtualisation (e.g., hypervisor) is not mentioned.
6.4	**Information security policy**	
6.4.2(b) Incremental	ISO/IEC 27001:2005 does not cover the development of a strategic plan although components of a strategic plan are covered. The Cloud Service Provider shall develop a strategic plan that includes a set of well defined roles and responsibilities for personnel with security responsibilities relevant to the design and implementation of cloud computing applications, databases, systems, network infrastructure and information processing that complies with policies, standards and applicable regulatory requirements.	Strategic plan was not explicitly mentioned. However, components of a possible strategic plan can be observed. Other requirements on strategic plan stated in ISO risk assessment standards are not fully met by ISO/IEC 27001:2005.
6.6	**Information security audits**	
6.6.2(a) Incremental	ISO/IEC 27001:2005 does not cover the establishment of an audit committee and the associated committee responsibilities. The Cloud Service Provider shall establish a formal / informal audit committee that contains, at a minimum, the members as stated in MTCS SS Clause 6.2.2(a). IT security audit plans shall also be approved by the abovementioned audit committee.	ISO/IEC 27001:2005 Sections 4.2.3 and 6.0 mention of undertaking regular reviews of the effectiveness of the ISMS, but no mention of a formal audit committee.
6.6.2(b) Incremental		Planning an ISMS audit in general, but no specific mention of approval process or audit committee.
6.6.2(c) Incremental	ISO/IEC 27001:2005 does not specify the frequency of IT security audits which shall be conducted at least once annually as per MTCS SS Clause 6.6.2(c). The Cloud Service Provider can opt to combine the audit activities with the audit conducted for traditional ISMS in conducting the abovementioned IT security audits at the required frequency.	Frequency of such audits not mentioned.
6.7	**Information security liaisons (ISL)**	
6.7.2(d) Incremental	ISO/IEC 27001:2005 does not specify the topics to be included in awareness and training sessions. The Cloud Service Provider shall include external industry risk development as one of the topics for awareness and training.	Awareness and training is present, but specific topic of external risk development not mentioned.
6.8	**Acceptable Usage**	

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
6.8.2(a) Incremental	ISO/IEC 27001:2005 does not require approval procedures and rules for acceptable usage for areas as stated in MTCS SS Clause 6.8.2(b). On top of the defined rules for the use of assets that is covered in ISO/IEC 27001:2005, the Cloud Service Provider shall define approval procedures for acceptable use policy.	Definition of rules for acceptable usage was mentioned but not details about approval process by authorised parties.
6.8.2(b) Incremental		Definition of rules for acceptable usage was mentioned but not details about specific authentication technology, service, device or company-approved product.
7	**Human resources**	
7.1	**Background screening**	
7.1.2(b) Incremental	ISO/IEC 27001:2005 does not cover specific areas and components where background checks should be conducted. While conducting background checks, the Cloud Service Provider shall ensure that the specific activities include areas and components as listed in MTCS SS Clause 7.1.2(b) upon initial hire for prospective employees and third parties that will have access to the information systems.	Components of background checks such as identity verification, character references, CV verification, criminal and credit checks not explicitly mentioned.
8	**Risk management**	
8.2	**Risk assessment**	
8.2.2(a) Incremental	ISO/IEC 27001:2005 does not consider cloud specific areas in the general ISMS risk assessments. Cloud Service Providers shall conduct risk assessments at least on an annual basis, or at planned intervals, or when there is significant change on any organisational control (e.g., security policies, procedures, standards), and system components relevant to the operation of the cloud services. Risk assessment shall be conducted in sufficient detail and covers the activities as stated in MTCS SS Clause 8.2.2(a), covering risk categories as stated in MTCS SS Clause 8.2.2(b), and including the likelihood and impact of all inherent and residual risks identified in MTCS SS Clause 8.2.2(c). As an additional reference for organisations seeking for certification in MTCS SS Level 3, see TR30:2012 *Technical Reference for Virtualisation security for servers* Annex A for a risk assessment worksheet on security in virtualisation.	Cloud specific risk assessment on threat and vulnerability assessment and impact assessment not mentioned.
8.2.2(b) Incremental		General ISMS risk assessment elements mentioned but do not include cloud specific areas.
8.2.2(c) Incremental		General ISMS risk assessment elements mentioned but do not include risk categories.
9	**Third party**	
9.1	**Third party due diligence**	

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
9.1.2(a) Incremental	ISO/IEC 27001:2005 does not cover specific areas (as stated in MTCS SS Clause 9.1.2(a)) to consider when performing due diligence before appointing a third party service provider to support the cloud environment. On top of identifying and addressing risks associated with third parties, the Cloud Service Provider shall understand and address the risks as stated in MTCS SS Clause 9.1.1. Cloud Service Providers shall carry out due diligence before appointing a third party service provider to determine the abovementioned areas. In this case, as defined in the MTCS SS, a third party service provider refers to a person, organisation or entity engaged by the Cloud Service Provider that supports the physical or logical cloud environment.	Identification and addressing of risks associated with third parties mentioned but not the specific criteria (e.g., viability, capability, track record).
9.4	**Third party delivery management**	
9.4.2(c) New	ISO/IEC 27001:2005 does not cover the implementation of security policies, procedures and controls by third party service providers supporting the cloud environment. The implementation of the above mentioned gap(s) shall also be at least as stringent as what the Cloud Service Provider would do for its own applicable operations.	Implementation of policies, procedures and controls is mentioned however the expectations on the extent of these components are not mentioned.
10	**Legal and compliance**	
10.1	**Compliance with regulatory and contractual requirements**	
10.1.2(b) New	ISO/IEC 27001:2005 does not cover requirements regarding cross-border movement and data transit. The Cloud Service Provider shall identify, create and maintain documentation that has taken into consideration, any cross-border and data transit requirements including statutory, regulatory, and contractual requirements applicable to the Cloud Service Provider. Some of the key areas to look into are location of data hosting, different regulation in hosting and user countries, and international standards.	Cloud specific requirements on cross-border movement and data transit were not mentioned.
10.1.2(d) New		Cloud specific requirements on cross-border movement and data transit were not mentioned.
10.2	**Compliance with policies and standards**	
10.2.2(a) Incremental	While ISO/IEC 27001:2005 covers review and audit activities in general, review and audit activities for cloud services may include additional elements. The Cloud Service Provider shall ensure that reviews and assessments include additional elements relevant to cloud technologies or the operation of the cloud services that the Cloud Service Provider is providing.	Review and audit for ISMS in general. Review and audit for cloud services may include additional elements.
10.3	**Prevention of misuse of cloud facilities**	

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
10.3.2(a) Incremental	While ISO/IEC 27001:2005 covers awareness and acceptable usage in general, specific components pertaining to the acceptable usage of the cloud environment, and the awareness of the monitoring policies, procedures and tools in place are not. Cloud Service Providers shall ensure that employees and third parties are aware of the precise scope of cloud environment's permitted access and use. Cloud Service Providers shall also include, in its awareness and training, topics pertaining to the abovementioned gaps that are relevant to cloud technology (e.g., acceptable usage, intrusion detection / prevention, content inspection).	Awareness and acceptable usage are mentioned but they are not specific to the cloud environment.
10.3.2(b) Incremental		Awareness in general mentioned but not specific topics about the monitoring features/controls in place.
10.3.2(c) New	ISO/IEC 27001:2005 does not cover the configuration of log-on warning messages or reminder on areas specified in MTCS SS Clause 10.3.2(c), and implementation of monitoring controls to detect if the cloud infrastructure is being used as a platform to attack others.	Specific requirement on log-on warning message or reminder on access policies and monitoring for accessing infrastructure or other privileged access are not mentioned.
10.3.2(d) New		Monitoring to detect if the cloud infrastructure is being used as a platform to attack others (e.g., nefarious use of cloud computing services) is not mentioned.
10.4	**Use of compliant cryptography controls**	
10.4.2(c) New	ISO/IEC 27001:2005 covers the usage of cryptographic control in general but not the application of prevailing industry practices in such controls. Cloud Service Providers shall apply prevailing industry practices, such as using industry standard ciphers and key lengths, while implementing and using cryptographic controls.	No specific mention of knowledge and application of prevailing industry practices.
10.6	**Continuous compliance monitoring**	
10.6.2(a) Incremental	ISO/IEC 27001:2005 does not cover the provision of continuous or real-time compliance monitoring. Cloud Service Providers shall implement a system configuration compliance reporting framework for the purposes as stated in MTCS SS Clause 10.6.2(a). In addition, the Cloud Service Provider shall also make event logs available for cloud users to perform monitoring.	Details on system configuration compliance reporting framework is not mentioned. Furthermore, details on the areas to be covered under configuration baselines and access matrices are not listed.
10.6.2(b) Incremental		Making logs available to cloud users for continuous and real-time monitor compliance not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
11	**Incident management**	
11.1	**Information security incident response plan and procedures**	
11.1.2(a) Incremental	While incident response is covered by ISO/IEC 27001:2005 in general, it does not cover additional areas with regards to the development of incident response plan and procedures. The Cloud Service Providers shall include areas as mentioned in MTCS SS Clause 11.1.2, specifically: • implementation of contact procedures • definition of the extent of cooperation in the Service Level Agreement (SLA) • escalation, recovery and resolution procedures / timeframes • incident severity levels and priorities • notification to customers about security breaches, including provision of digital forensic evidences, as required.	Roles and responsibilities mentioned but not specific to CSPs or relevant parties. Consider incident response as part of business continuity.
11.1.2(b) Incremental		Implementation of contact procedures was not explicitly mentioned.
11.1.2(c) New		Definition of the extent of cooperation in the Service Level Agreement (SLA) was not mentioned.
11.1.2(e) Incremental		Incident response in general mentioned but not the escalation, recovery and resolution procedures/time frames. Consider incident response as part of business continuity.
11.1.2(g) Incremental		Quantification and monitoring mentioned but not classification by severity levels and priorities.
11.1.2(h) Incremental		Notification to customers about any security breach is not mentioned.
11.1.2(i) Incremental		Collection of evidence mentioned but not the capability to provide consumers with evidence.
11.2	**Information security incident response plan testing and updates**	
11.2.2(a) Incremental	While incident response is covered by ISO/IEC 27001:2005 in general, ISO/IEC 27001:2005 does not cover areas with regards to the testing and update of incident response plan and procedures as stated in MTCS SS Clause 11.2.2, especially on test plan for incident response plan, frequency of testing of the incident response plan (annual) and testing responsibilities. The Cloud Service Provider shall include types of	No mention of test plan for incident response plan. Consider incident response as part of business continuity.
11.2.2(b) New		No mention of the frequency of testing for the incident response plan.

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
11.2.2(c) Incremental	tests, test scope and parties to be involved in the test execution and review in an incident response test plan. In addition, appropriate training shall be given to personnel assigned with information security incident response responsibilities.	Security training in general and not specific to incident response responsibilities. Consider incident response as part of business continuity.
11.3	**Information security incident reporting**	
11.3.2(b) Incremental	While ISO/IEC 27001:2005 mentions reporting of information security events through appropriate management channels, it does not cover details related to notification and support to users. The Cloud Service Providers shall include the notification and provision of support, in a timely manner, to the relevant cloud users and third parties affected by the security breach.	While reporting of information security events through appropriate management channels is mentioned, notification specific to customers and affected third parties about the security breach is not mentioned.
11.4	**Problem management**	
11.4.2(c) Incremental	ISO/IEC 27001:2005 does not cover the establishment of escalation processes for problems with different severity levels. Cloud Service Providers shall include escalation procedures and processes in addition to the risk treatment plan defined in ISO/IEC 27001:2005 Clauses 4.2.1 and 4.2.2. These incidents can include information security and non-information security incidents. In addition, Cloud Service Providers shall also ensure that relevant management approval for these escalation processes is obtained.	Establishment of escalation process for problems with different severity levels not explicitly mentioned though risk treatment plans could include an escalation process/procedure.
12	**Data Governance**	
12.5	**Data protection**	
12.5.2(a) Incremental	ISO/IEC 27001:2005 does not cover specific media handling for virtualised images and snapshots. On top of the media handling controls and procedures mentioned in ISO/IEC 27001:2005 Clause A.10.7, Cloud Service Providers shall establish controls and procedures to protect data from loss and destruction and implement security controls over access to all media (as stated in MTCS SS Clause 12.5.2(a)), including virtualised images and snapshots.	Media is mentioned in general. However, specific media, virtualised images and snapshots are not mentioned.
12.7	**Data backups**	
12.7.2(b) Incremental	While ISO/IEC 27001:2005 covers backups in general, the frequency of testing required on these backups, and the access and storage locations of	Backups are mentioned in general but not the frequency of the testing of backups.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
12.7.2(c) Incremental	these backups are not covered. Cloud Service Providers shall include the abovementioned requirements on top of the existing backup requirements in ISO/IEC 27001:2005 Clauses A.10.5 and A.9.2.	Backups and security of equipment off premises mentioned in general but not procedures to determine access and storage locations of backups.
12.8	**Secure disposal and decommissioning of hardcopy, media and equipment**	
12.8.2(c) New	ISO/IEC 27001:2005 does not specifically cover the secure disposal and decommissioning procedures of hardcopy materials. Cloud Service Providers shall establish secure disposal procedures for the hardcopy, media and equipment, which include methods as stated in MTCS SS Clause 12.8.2(c), so that data cannot be reconstructed or obtain a "Certificate of Destruction" from a data disposal third party as evidence of secure disposal.	Specific procedures to securely dispose hardcopy materials containing data are not mentioned.
13	**Audit logging and monitoring**	
13.1	**Logging and monitoring process**	
13.1.2(f) Incremental	While ISO/IEC 27001:2005 covers audit logging and log review in general, it does not cover specifically requirement as stated in MTCS SS Clause 13.1.2(f). As part of log reviews performed, the Cloud Service Provider shall review usage of identification and authentication methods. In addition, they shall review instances of audit trails being initialised.	Audit logging and log review mentioned in general, not specific to logging and review of identification / authentication mechanism usage.
13.3	**Audit trails**	
13.3.2(a) Incremental	While ISO/IEC 27001:2005 covers audit trails, it does not cover the level of details to be captured in audit trails. The level of details to be captured is as stated in MTCS SS Clause 13.3.2(a).	Audit trail mentioned in general, but specific details captured are not mentioned.
13.5	**Usage logs**	
13.5.2(a) Incremental	While ISO/IEC 27001:2005 covers the protection of logs in general, it does not specifically cover the protection of usage logs using strict files and directories' permissions. The Cloud Service Provider shall ensure that the usage logs are protected against modification.	Protection of logs in general is mentioned but not specifically having strict files and directories' permissions.
14	**Secure configuration**	
14.1	**Server and network device configuration standards**	
14.1.2(a - e) Incremental	ISO/IEC 27001:2005 does not cover detailed components of the network security management and controls implementation. Refer to MTCS SS Clause 14.1.2 for specific requirements regarding server and network device configuration standards.	Network security management and controls implementation in general although details are not mentioned.
14.2	**Malicious code prevention**	

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
14.2.2(b - f) Incremental	ISO/IEC 27001:2005 does not cover specific control requirements for malicious code prevention on top of the controls mentioned in ISO/IEC 27001:2005 Clause A.10.4. Refer to MTCS SS Clause 14.2.2 for specific control requirements to address malicious code prevention. Also the Cloud Service Provider shall include appropriate awareness procedures for the administrators of cloud systems in its awareness and training.	Controls against malicious codes are mentioned but specific requirements are not mentioned.
14.2.2(g) Incremental		Awareness in general is mentioned, specific topics for administrations of cloud systems not mentioned.
14.4	**Physical port protection**	
14.4.2(b) Incremental	ISO/IEC 27001:2005 Clause A.11.4 covers physical port protection but specific network configuration and control are missing. The Cloud Service Provider shall disable all ports (both physical and logical) and remove the configurations of unused ports (both physical and logical) and implement configurations necessary for the hardening of these ports.	"Physical and logical access to diagnostic and configuration ports shall be controlled" partially covers the requirement.
14.4.2(c) Incremental		"Physical and logical access to diagnostic and configuration ports shall be controlled" partially covers the requirement.
14.7	**Unnecessary service and protocols**	
14.7.2(a) Incremental	ISO/IEC 27001:2005 does not cover the detailed configurations of system security parameters to prevent the misuse of services and protocols as mentioned in MTCS SS Clause 14.7.2. The Cloud Service Provider shall also maintain a log to monitor services and protocols enablement / disablement.	Network security mentioned in general although details are not mentioned.
14.7.2(b) Incremental		Network security mentioned in general although details are not mentioned.
14.7.2(c) Incremental		Network security mentioned in general although details are not mentioned.
15	**Security testing and monitoring**	
15.1	**Vulnerability scanning**	
15.1.2(a) Incremental	ISO/IEC 27001:2005 does not cover details of vulnerability (both internal and external) scanning as stated in MTCS SS Clause 15.1.2. Cloud Service Providers shall conduct vulnerability scanning at least on quarterly basis. They must address vulnerabilities with a Common Vulnerability Scoring System (CVSS) base score of 7-10 within one week. CVSS is an industry open standard designed to convey vulnerability severity and helps determine urgency and priority of response. Cloud Service Providers are recommended to adopt the CVSS standard for rating vulnerabilities.	Identification of vulnerabilities is mentioned, but specific usage of vulnerability scanning is not. Frequency of such scans is also not mentioned.
15.1.2(b) Incremental		Evaluation of vulnerabilities and implementation of controls to address vulnerabilities are mentioned in general. Usage of CVSS scoring and the addressing vulnerabilities within one week are not mentioned.
15.2	**Penetration testing**	

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
15.2.2(a) New	ISO/IEC 27001:2005 does not explicitly cover penetration testing. Network layer and application layer penetration testing from locations as specified in MTCS SS Clause 15.2.1 shall be conducted by the Cloud Service Provider at least on an annual basis, and maintain logs and reports of penetration tests conducted and follow-up actions.	Penetration testing is not mentioned in ISO/IEC 27001:2005.
15.3	**Security monitoring**	
15.3.2(b) New	ISO/IEC 27001:2005 does not cover intrusion detection and prevention systems (IDPS). Cloud Service Providers shall implement IDPS to monitor traffic, and establish and maintain up-to-date policies on security principles for network intrusion, detection and prevention to complement the IDPS implemented.	Implementation of intrusion detection systems and/or intrusion prevention systems not mentioned.
15.3.2(c) Incremental		Specific topics about network intrusion, detection and prevention are not mentioned.
16	**System acquisitions and development**	
16.1	**Development, acquisition and release management**	
16.1.2(a) Incremental	While ISO/IEC 27001:2005 Clauses A.12, A.6.2 and A.10.1 cover the consideration of security principles in general during the system development life cycle, it does not include additional details relevant to the development and acquisition of components as stated in MTCS SS Clause 16.1.1. On top of taking into account security principles, Cloud Service Providers shall develop applications (both internal and external) while adhering to and verifying with industry accepted practices / standards. Cloud Service Providers shall enforce proper approvals for any changes, to components as stated in MTCS SS Clause 16.1.1, prior to the implementation, maintain reports and documentation of any changes, remove components as stated in MTCS SS Clauses 16.1.2(b) and 16.1.2(c) before production systems become active. Additionally, procedures and controls relevant to the development and acquisition of components as stated in MTCS SS Clause 16.1.1 shall also be included in the Cloud Service Provider's policies that are relevant to system acquisitions and development.	Development of applications in accordance with industry accepted practices is not mentioned though security principles are included during the system development life cycle (SDLC) phase under ISO/IEC 27001:2005 Section A.12.1.1.
16.1.2(b) Incremental		Addressing security requirements before giving access to customers mentioned but not the specific actions (e.g., removal of custom accounts, IDs and passwords).
16.1.2(c) Incremental		Removal of test data and accounts is not mentioned.
16.1.2(d) Incremental		Security principles are included during the SDLC phase under ISO/IEC 27001:2005 Section A.12.1.1 but verification against industry standards is not mentioned.
16.1.2(j) New		N.A
16.1.2(k) New		N.A
16.1.2(l) New		N.A

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
16.4	**Source code security**	
16.4.2(a) Incremental	While ISO/IEC 27001:2005 Clause A.12.4.3 covers access control to program source code, version control is not included. The Cloud Service Provider shall enforce version control on all custom developed software. If the development of such software is done by an external party, the Cloud Service Provider must perform its due diligence to ensure that the external party enforces version control during the development process.	Enforcement of version control is not mentioned.
17	**Encryption**	
17.1	**Encryption policies and procedures**	
17.1.2(a) Incremental	While ISO/IEC 27001:2005 Clause A.12.3 covers the usage of cryptographic controls in general, the need to document, in policies and procedures, specific components as stated in MTCS SS Clause 17.1.2(a) is not included. The Cloud Service Provider shall ensure that policies and procedures have taken into consideration components as stated in MTCS SS Clause 17.1.2(a) and also ensure that these documentations are approved by the management, and reviewed and updated periodically.	Usage of cryptography controls mentioned in general but specific topics are not.
17.1.2(b) Incremental	ISO/IEC 27001:2005 does not cover specific usage of encryption as stated in MTCS SS Clause 17.1.2(b). The Cloud Service Provider shall: • apply encryption policies to sensitive information in-transit and in-storage • ensure that policies are approved by the management • review and update documents periodically	While protection of information is mentioned, the specific usage of encryption is not.
17.2	**Channel encryption**	
17.2.2(a) Incremental	ISO/IEC 27001:2005 does not cover specific usage of encryption as stated in MTCS SS Clause 17.2.2(a). The Cloud Service Provider shall implement encryption (where applicable) for all non-console administrative access.	Usage of cryptography in general is mentioned but not specifically for non-console administrative access.
17.3	**Key management**	
17.3.2(a) Incremental	ISO/IEC 27001:2005 does not cover areas relevant to the lifecycle of cryptographic keys (from generation to destruction). The Cloud Service Provider shall establish policies and procedures relevant to the stages (as stated in MTCSS SS Clause 17.3.1) of the cryptographic key lifecycle, specifically the storage, distribution and change procedures of these keys. The Cloud Service Provider shall also	Policy on use of cryptography mentioned in general.
17.3.2(b) Incremental		Policy on use of cryptography mentioned in general.
17.3.2(c) Incremental		Key changing procedures are not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
17.3.2(d) Incremental	ensure that formal acknowledgement of responsibilities is given by custodians of these cryptographic keys.	Formal acknowledgement of responsibilities is not mentioned.
17.4	**Electronic messaging security**	
17.4.2(b) Incremental	While ISO/IEC 27001:2005 Clause A.10.8 covers security of information exchange, specific area as stated in MTCS SS Clause 17.4.2(b) is not included. Cloud Service Providers shall ensure that the transportation and addressing of information involved in electronic messaging are sufficiently protected and accurately transmitted.	Information exchange policies, procedures and controls in general. Specific requirement is not mentioned though it could be included in the policies, procedures and controls.
17.4.2(c) New	ISO/IEC 27001:2005 does not cover the usage and control of less-secure messaging systems. The Cloud Service Provider shall ensure that less-secure messaging systems are limited and controlled.	Control of usage of less-secure messaging systems is not mentioned.
17.4.2(d) Incremental	While ISO/IEC 27001:2005 Clause A.10.8 covers security of information exchange, the specific control as stated in MTCS SS Clause 17.4.2(d) is not included. Cloud Service Providers shall ensure that stronger levels of authentication and message content protection are in place when public networks are being used as the medium of communication of information.	Implementation of stronger controls when using public networks is not mentioned.
17.4.2(e) New	ISO/IEC 27001:2005 does not cover the usage of open standards to manage email spoofing. The Cloud Service Provider shall ensure that open standards (e.g., Send Policy Framework, DomainKey (DKIM)) are used to manage email spoofing.	Usage of open standards to prevent and detect spoof emails is not mentioned.
17.4.2(f) Incremental	While ISO/IEC 27001:2005 Clauses A.10.8 and A.12.2 cover security for electronic messaging, specific component as stated in MTCS SS Clause 17.4.2(f) are not included. Cloud Service Providers shall ensure that digital signatures are being used on emails to secure email communications between them and the cloud users.	Implementation and usage of digital signatures is not mentioned.
18	**Physical and environmental**	
18.1	**Asset management**	
18.1.2(c) Incremental	While ISO/IEC 27001:2005 covers equipment security and support for equipments in general, it does not cover the need to have applicable redundancies to protect equipments of the nature as stated in MTCS SS Clause 18.1.2(c). Cloud Service Providers shall ensure that the abovementioned equipments have applicable redundancies to protect them from power failures based on their risk of failure.	Usage of applicable redundancies is not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
18.1.2(d) New	While ISO/IEC 27001:2005 Clause A.9.2.3 covers the protection of cables, disconnection of hardware devices from the network is not covered. Cloud Service Providers shall ensure that unused hardware devices are disconnected from the network.	Protection of cables is mentioned under ISO/IEC 27001:2005 Section A.9.2.3 but disconnection of unused devices is not.
18.3	**Physical access**	
18.3.2(b) Incremental	While elements of physical security are present in ISO/IEC 27001:2005 Clause A.9.1, it does not include requirement specific to surveillance. On top of the physical security elements, Cloud Service Providers shall implement surveillance systems that will monitor access to and within the information storage and processing facilities.	Physical security elements are present but surveillance is not explicitly mentioned.
18.3.2(e) Incremental	While ISO/IEC 27001:2005 Clause A.8.3.3 covers the removal of access rights, the concept of granting access rights is not specifically covered. The Cloud Service Provider shall grant access rights to authorised personnel (internal or external parties) on a need basis and ensure that these personnel do not have more rights than needed to perform their roles.	Access granting on a need basis is not mentioned.
18.4	**Visitors**	
18.4.2(a) Incremental	While ISO/IEC 27001:2005 Clauses A.9.1 and A.10.6 cover physical security elements, requirements pertaining to external visitors as stated in MTCS SS Clause 18.4 are not covered. The Cloud Service Provider shall ensure that visitors to facilities are accompanied by an authorised personnel and the temporary visitation pass or badge that they receive shall also be differentiated from the ones that personnel on-site possess. In addition, network points that can be accessed by visitors shall be appropriately managed and controlled to prevent authorised usage.	Escort by authorised personnel to the facility is not mentioned.
18.4.2(b) Incremental		Having physical security controls in place would imply having requiring pass/badge for access but differentiation between visitors and on-site personnel is not mentioned.
18.4.2(d) New		ISO/IEC 27001:2005 Section 4.3.3 mentioned having a visitors' log but reviewing of such log is not mentioned.
18.4.2(e) Incremental		Management and control of networks are mentioned but specific restriction on publicly accessible network points is not.
18.5	**Environmental threats and equipment power failures**	
18.5.2(b) New	While ISO/IEC 27001:2005 Clauses A.9.1 and A.9.2 include elements of equipment security and protection of equipment from environmental threats, specific measures and controls, as stated in MTCS SS Clause 18.5.2, to be implemented are not included. The Cloud Service Provider shall ensure that tamper proofing is done by external parties and	Tamper proofing by external parties is not mentioned.
18.5.2(c) Incremental		Protection of equipment from environment threats and hazards is mentioned but not maintaining/monitoring of temperature.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
18.5.2(d) Incremental	not themselves. Measures shall be in place to maintain and monitor temperature and humidity levels in the information storage and processing facilities. Systems relevant to fire protection and suppression shall be installed and maintained regularly. The Cloud Service Provider shall also ensure that sufficient measures and controls are in place to prevent utility service outages and power surges. The details of these implementations shall commensurate with the service level commitments and risks of utility issues.	Specific measures against fire are not mentioned.
18.5.2(f) Incremental		Protection from power failures mentioned in general but not specific security mechanisms, redundancies, alternative power source and alternative routing.
18.5.2(g) Incremental		Protection from the effects of large amount of systems being turned on is not mentioned.
18.5.2(h) Incremental		Protection from power failures mentioned but not the commensuration of protection with service level commitments.
18.6	**Physical security review**	
18.6.2(a) Incremental	Reviews are covered by ISO/IEC 27001:2005 Clause 4.2.3 in general but the frequency of such reviews and the specific physical reviews (as stated in MTCS SS Clause 18.6.2(a)) to be performed are not included. The Cloud Service Provider shall perform a review of physical security controls at least on an annual basis and this review shall cover specific components as stated in MTCS SS Clause 18.6.2(a). Cloud Service Providers can opt to combine such reviews with the traditional ISMS reviews by expanding on the scope of these reviews to include specific physical security areas.	Review of ISMS in general. While physical security elements are present, review of physical security controls and procedures is not.
18.6.2(b) Incremental		Review of ISMS in general, specific frequency is not mentioned.
19	**Operations**	
19.2	**Documentation of service operations and external dependencies**	
19.2.2(a) Incremental	ISO/IEC 27001:2005 does not cover cloud specific documentations. Proper and complete documentation and assessment of the service operations shall be ensured by the Cloud Service Provider. These documentations shall also be kept complete and up-to-date by the Cloud Service Provider to include areas as stated in MTCS SS Clause 19.2.2(a).	While not specific to cloud services, this clause is about documentations in general which is adequately covered in ISO/IEC 27001:2005.
19.3	**Capacity management**	
19.3.2(a) Incremental	While ISO/IEC 27001:2005 Clause A.9.2 covers the availability and quality of resources, specifics of capacity management are not covered. The Cloud Service Provider shall establish a plan or process to monitor and plan capacity and resource requirements in order to ensure system and service performance as committed can be delivered.	Availability and quality of resources is covered under ISO/IEC 27001:2005 Section A.9.2.4 but not capacity is not.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
20	**Change management**	
20.2	**Backup procedures**	
20.2.2(a) Incremental	While ISO/IEC 27001:2005 Clauses A.10.1, A.10.2 and A.10.5 covers backups and change management in general, the requirement to perform backups for systems specifically prior to modifying them is not included. The Cloud Service Provider shall perform backups for systems or applications before any changes are applied to them. However, if the change has been tested in an environment that mirrors the production environment, such backups need not be performed though Cloud Service Providers are still encouraged to. In this case, changes include those performed for components of the cloud infrastructure. Examples of changes include system and security configuration changes, hardware devices and security patches, software updates, and creation, storage and use of virtualised images and snapshots.	ISO/IEC 27001:2005 covers back-up in general; however, performing backups specifically for systems / applications prior to change is not mentioned.
20.5	**Patch management procedures**	
20.5.2(a) Incremental	ISO/IEC 27001:2005 does not cover patch management procedures and configurations to be applied to dormant / offline systems for hardening purposes. A patch management process shall be put in place by the Cloud Service Provider. This process shall be kept updated and relevant. The Cloud Service Provider shall also ensure that configurations for hardening purposes are applied to systems that have been dormant / offline for a period of time so that these systems are secured similarly to systems that have already been active before being deployed or connected to the network.	Implementation of patch management procedures is not mentioned.
20.5.2(b) Incremental		Implementation of a process to manage systems that have been dormant/offline is not mentioned.
21	**Business continuity planning (BCP) and disaster recovery (DR)**	
21.2	**BCP and DR plans**	
21.2.2(a) Incremental	ISO/IEC 27001:2005 does not explicitly cover disaster recovery though components of it exist in business continuity-related areas. In addition to business continuity elements in ISO/IEC 27001:2005 Clause A.14.1, plans for BCP and DR shall be developed and implemented by the Cloud Service Provider.	Disaster recovery is not mentioned in ISO/IEC 27001:2005 though elements of it can be found in business continuity planning-related clauses.

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
21.2.2(b) Incremental	These plans shall include, but not be limited to, the requirements defined in MTCS SS Clause 21.2.2. While developing these plans, risk assessments shall be conducted to identify and evaluate events that can interrupt normal operations. The risk assessments shall also evaluate if BCP and DR plans are necessary for components of the cloud services depending on their criticality. In these plans, Cloud Service Providers shall also establish detailed roles and responsibilities for personnel that are to be involved.	Roles and responsibilities not explicitly mentioned but could be included in the business continuity planning (BCP) / disaster recovery (DR) planning process and framework.
21.3	**BCP and DR testing**	
21.3.2(a) Incremental	ISO/IEC 27001:2005 does not cover disaster recovery components. On top of the business continuity mentioned in ISO/IEC 27001:2005 Clause A.14.1, BCP and DR plans shall be developed and implemented by the Cloud Service Provider. The Cloud Service Provider shall implement a process to test, validate and update business continuity and disaster recovery plans regularly to ensure adequacy and effectiveness of recovery requirements, and personnel's ability to execute emergency and recovery procedures.	Disaster recovery is not mentioned in ISO/IEC 27001:2005 though elements of it can be found in business continuity planning-related clauses.
22	**Cloud services administration**	
22.1	**Privilege account creation**	
22.1.2(c) Incremental	ISO/IEC 27001:2005 does not cover privileged accounts. While ISO/IEC 27001:2005 Clauses A.11.1 and A.11.2 covers access granting procedures, granting and modifying access to cloud components (as stated in MTCS SS Clause 22.1.2(c)) may entail additional details. The Cloud Service Provider shall establish a process for granting of accounts with access to the above mentioned cloud components and ensure that management approval is obtained. In addition, the Cloud Service Provider shall ensure that these privileged accounts are not used as system or service accounts. In this case, these accounts refer to accounts belonging to personnel administering the cloud services (e.g., applications, systems, databases, network configurations, and sensitive data and functions).	Access granting procedures could be included in access control policy. While this clause has cloud-specific components in it, it has the same context as traditional ISMS and technology environments.
22.1.2(d) New		Privileged accounts are not mentioned.
22.2	**Generation of administrator passwords**	

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
22.2.2(a) Incremental	ISO/IEC 27001:2005 does not cover specific criteria for administrator passwords. Cloud Service Providers shall ensure that minimum password criteria follow industry standard practices as stated in MTCS SS Clause 22.2.2(a). In addition, Cloud Service Providers shall disallow generic passwords via system and application configuration as well as prepare documentation on minimum password criteria, and shared passwords with other accounts.	Good security practices for passwords are mentioned in general. Specific password criteria are not mentioned.
22.2.2(b) Incremental		Good security practices for passwords are mentioned in general.
22.2.2(c) Incremental		Good security practices for passwords are mentioned in general.
22.3	**Administrator access review and revocation**	
22.3.2(c) Incremental	While ISO/IEC 27001:2005 Clause 11.2.4 covers the review and removal of access rights, the specific frequency to perform such review is not. A formal access review and revocation process shall be established by the Cloud Service Provider to review the adequacy of privileges and access levels, and de-provision or remove access in a timely manner, which includes removal or disabling of inactive accounts at least every ninety (90) days and notify the relevant parties of the action taken above.	Removal or disabling of inactive accounts could be part of the review process. Specific frequency is not mentioned.
22.4	**Account lockout**	
22.4.2(a) New	ISO/IEC 27001:2005 does not cover account lockout. A formal process to detect and terminate unauthorised access attempts in a timely manner shall be implemented by the Cloud Service Provider. Account lockout requirements shall also be established based on the risk assessments and sensitivity of the system and data. Minimally, the requirements defined in MTCS SS Clause 22.4.2 shall be implemented.	Account lockout and lockout criteria are not mentioned in ISO/IEC 27001:2005.
22.4.2(b) New		Account lockout and lockout duration are not mentioned in ISO/IEC 27001:2005.
22.5	**Password change**	
22.5.2(a) New	While ISO/IEC 27001:2005 Clause 11.3 covers some elements of password change, details as stated in MTCS SS Clause 22.5.2 are not included. The Cloud Service Provider shall enforce compulsory password change based on industry standard practices. The new passwords should also satisfy the requirement as stated in MTCS SS Clause 22.5.2(b).	Enforcement of compulsory password change is not mentioned.
22.5.2(b) Incremental		Password history requirement is not mentioned.
22.6	**Password reset and first logon**	
22.6.2(a) Incremental	ISO/IEC 27001:2005 does not cover details on password reset and change, and two-factor authentication (2FA). Firstly, the Cloud Service Provider shall ensure that unique passwords are	Generation of unique passwords and mandatory password change upon first login are not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
22.6.2(b) Incremental	generated and users are required to change their passwords upon first login. Secondly, when changing passwords, users shall also be required to verify their identity before password change is continue or processed. Thirdly, management approval shall be obtained when a password reset is requested. Fourthly, in the event that the 2FA device is lost, the password shall be reset.	Verification of identity prior to changing password is not mentioned.
22.6.2(c) Incremental		Management approval for password reset is not mentioned.
22.6.2(d) New		2FA is not mentioned in ISO/IEC 27001:2005.
22.7	**Administrator access security**	
22.7.2(d) New	ISO/IEC 27001:2005 does not cover enablement for administrative rights and role-based access control (RBAC). The Cloud Service Provider shall ensure that explicit approval is obtained if local administrative access is enabled or required, and RBAC mechanisms are in place to control administrative access.	Explicit approval for enablement of administrative rights is not mentioned.
22.7.2(e) Incremental		RBAC mechanisms are not mentioned.
22.8	**Administrator access logs**	
22.8.2(a) New	ISO/IEC 27001:2005 does not cover establishment of procedures to review administrator activities. The Cloud Service Provider shall log via native systems or application logs for all administrator activities (as stated in MTCS SS Clause 12), and establish a procedure to review all administrator activities periodically.	Procedure to review administrator activities is not mentioned.
22.9	**Session management**	
22.9.2(b) Incremental	While ISO/IEC 27001:2005 A.11.5.5 covers the timing out of sessions, it does not cover the requirement as stated in MTCS SS Clause 22.9.2(b). Configurations shall be put into place by the Cloud Service Provider to lock the user session after an idle time of more than fifteen (15) minutes. Users shall also be required to re-enter their passwords in order to reactivate the session. In addition, the Cloud Service Provider shall also ensure that the hardening documents are approved by relevant management and contains the requirements as stated in MTCS SS Clause 22.9.2.	Requirement to re-enter password after session idle is not mentioned. Specific period of idling is also not mentioned.
22.10	**Segregation of duties**	
22.10.2(a) Incremental	While ISO/IEC 27001:2005 covers the review of user access rights and the segregation of duties, the specific frequency of such reviews is not included. The Cloud Service Provider shall ensure that the review of access rights and segregation of duties is done at least on an annual basis. The Cloud Service Provider shall also ensure that individuals are	Specific frequency of review is not mentioned.
22.10.2(b) Incremental		Movement of object codes between environments is not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
22.10.2(c) Incremental	restricted from moving object codes between environments (i.e., from development to production). Individuals shall also be restricted from accessing backup and production systems.	Separation of environments mentioned but not restriction of access to backup and production systems.
22.11	**Secure transmission of access credentials**	
22.11.2(a) New	ISO/IEC 27001:2005 does not cover the usage of no clear-text protocols. Appropriate encryption (based on requirements in MTCS SS Clause 16) and security protocols shall be implemented by the Cloud Service Provider for transmitting credentials for non-console administrative access based on the risk assessments and sensitivity of the system and data.	Usage of no clear-text protocols for administrative access is not mentioned in ISO/IEC 27001:2005.
22.12	**Third party administrative access**	
22.12.2(a) Incremental	ISO/IEC 27001:2005 does not cover the granting of access to vendors. The Cloud Service Provider shall ensure that privileged access granted to vendors is based on a "need-to-have" basis.	Granting access on a need-to-have basis is not mentioned.
22.13	**Service and application accounts**	
22.13.2(a) Incremental	ISO/IEC 27001:2005 Clause A.11.2 does not cover details on service and application accounts, the Cloud Service Provider shall ensure that all service and application accounts are created in accordance with the requirements as stated in MTCS SS Clause 22.13.2(a).	Service and application accounts not explicitly mentioned.
23	**Cloud user access**	
23.2	**User access security**	
23.2.2(a) Incremental	ISO/IEC 27001:2005 does not cover details on documented approval, having a default “deny all” setting and having anti-bot controls in place. The Cloud Service Provider shall enforce: • documented approval from authorised personnel for the granting of user access privileges • default "deny-all" setting • implementation of anti-bot controls There are two components of cloud user access: cloud user’s administrator who manages its own environment via an administrative interface, and end users who access the systems to use specific cloud services.	Enforcement of documented approval from authorised personnel not mentioned.
23.2.2(c) New		"Deny-all" setting is not mentioned.
23.2.2(e) New		Implementation of anti-bot controls is not mentioned.
23.3	**User access password**	
23.3.2(a) Incremental	While ISO/IEC 27001:2005 Clause A.11.3 covers user access password, specific password criteria as stated in MTCS SS Clause 23.3.2(a) are not mentioned. The Cloud Service Provider shall ensure that generic passwords are not allowed and passwords cannot be shared among accounts.	Specific password criteria are not mentioned in ISO/IEC 27001:2005.
23.3.2(b) Incremental		Good security practices for passwords are mentioned in general.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
23.3.2(c) Incremental		Good security practices for passwords are mentioned in general.
23.4	**User account lockout**	
23.4.2(a) New	ISO/IEC 27001:2005 does not cover details on account lockout. The Cloud Service Provider shall put into place configurations or measures to lock user accounts out after criteria as stated in MTCS SS Clause 23.4.2 are satisfied. Reviews shall also be conducted by the Cloud Service Provider to ensure that configurations have been put into place in accordance with hardening documents approved beforehand.	Account lockout criteria are not mentioned in ISO/IEC 27001:2005.
23.4.2(b) New		Account lockout duration is not mentioned in ISO/IEC 27001:2005.
23.5	**User password reset and 1st logon change**	
23.5.2(a) Incremental	ISO/IEC 27001:2005 does not cover details on password reset and change. Firstly, the Cloud Service Provider shall ensure that unique passwords are generated and users are required to change their passwords upon first login. Secondly, when changing passwords, users shall also be required to verify their identity before password reset is processed.	Generation of unique passwords and mandatory password change upon first login are not mentioned.
23.5.2(b) Incremental		Verification of user identity in the event of a password reset is not mentioned.
23.6	**Password protection**	
23.6.2(a) Incremental	ISO/IEC 27001:2005 Clauses A.10.8 and A.12.3 covers information exchange policies and the usage of cryptographic controls but specific control as stated in MTCS SS Clause 23.6.2 is not included. The Cloud Service Provider shall ensure that all passwords are rendered unreadable during transmission. The channels where the transmission is performed shall also be encrypted. In addition, the Cloud Service Provider shall sufficiently protect the passwords by encrypting the password storage.	Rendering passwords unreadable during transmission not explicitly mentioned.
23.6.2(b) Incremental		Information exchange policies, procedures and controls in general. Usage of encrypted channels could be included in exchange policies.
23.6.2(c) New		Password storage is not mentioned in ISO/IEC 27001:2005.
23.7	**User session management**	
23.7.2(b) Incremental	While ISO/IEC 27001:2005 Clause 11.5.5 covers the timing out of user sessions upon inactivity, it does not define the period of inactivity to consider and the need for users to re-enter their passwords to reactivate the system. The Cloud Service Provider shall configure the systems such that sessions are locked out upon an idle time of more than fifteen (15) minutes and users will be required to re-enter their passwords in order to reactivate the system.	Requirement to re-enter password after session idle is not mentioned. Specific period of idling is also not mentioned.

MTCS SS Level 1 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
23.7.2(c) Incremental	Cryptographically strong session identifiers shall be implemented.	Implementation of cryptographically strong session identifiers is not mentioned.
23.9	**Self-service portal creation and management of user accounts**	
23.9.2(a) Incremental	While ISO/IEC 27001:2005 Clause 11.3 covers elements of good security practices for passwords, it does not cover specific criteria for self-service portals. The Cloud Service Provider shall maintain strict password criteria in accordance to requirements as defined in MTCS SS Clause 23.3.	Good security practices for passwords mentioned in general. Specific password criteria are not mentioned in ISO/IEC 27001:2005.
23.10	**Communication with cloud users**	
23.10.2(a) New	ISO/IEC 27001:2005 does not cover the security of the distribution of official notifications. The Cloud Service Provider shall implement communication mechanisms to communicate official notifications securely to cloud users.	Security of notifications is not mentioned.
24	**Tenancy and customer isolation**	
24.1	**Multi tenancy**	
24.1.2(c) Incremental	While ISO/IEC 27001:2005 Clause A.11.4.5 covers segregation of networks, does not cover segregation details for components relevant to virtualisation. The Cloud Service Provider shall enforce segregation between virtual machines belonging to different users to prevent contagion effect of changes applied to a specific user's virtual machine from spreading to other users' virtual machines.	Segregation of networks in general is mentioned. However, virtual machines are not mentioned in ISO/IEC 27001:2005.
24.3	**Network protection**	
24.3.2(d) Incremental	ISO/IEC 27001:2005 does not cover network protection details for the cloud infrastructure. Secure network architecture shall be designed, implemented and managed by the Cloud Service Provider to protect the cloud infrastructure. A test plan shall also be formulated to verify and assess the implemented measures, develop compensating controls and ensure the network is protected. Minimally, the requirements as defined in MTCS SS Clause 24.3.2 shall be in place: • compare critical network infrastructure configurations against standards for each type of network device and ensure that any deviations from the baselines are managed and controlled • review the network environment at regular	Comparison of network configurations against standards not mentioned.
24.3.2(e) New		Review of network environment is not mentioned.
24.3.2(f) Incremental		Identification of risks related to data flow network architecture not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
24.3.2(j) New	planned intervals • identify high-risk environments and data flow network architecture diagrams that may have impact on the organisation's compliance to regulations •implement multi-factor authentication for all remote user access In this case, remote user access mentioned above is relevant for all cloud users (e.g., end users). The Cloud Service Provider shall also restrict access to virtualisation layer, including the hypervisor management software and implement multi-factor and / or split control authentication to restrict access to hypervisor and disable remote management of hypervisor for cloud implementation using virtualisation technology.	Multi-factor authentication is not mentioned in ISO/IEC 27001:2005.
24.3.2(k) New		Virtualisation layer is not mentioned in ISO/IEC 27001:2005.
24.3.2(l) New		Multi-factor authentication and split control authentication are not mentioned in ISO/IEC 27001:2005.
24.4	**Virtualisation**	
24.4.2(a) Incremental	ISO/IEC 27001:2005 does not cover security requirements specific to virtualisation components and systems. Information security risks that may arise from the deployment of virtualisation technology for the cloud environment shall be assessed and managed by the Cloud Service Provider. The Cloud Service Provider shall identify security risks including, but not limited to, those as stated in MTCS SS Clause 24.4.2(a), and address them. While ISO/IEC 27001:2005 Clause 4.2.1 covers risk assessment and risk treatment in general, risk assessment and risk treatment specific for	Specific VM-related features, risks and configurations are not mentioned in ISO/IEC 27001:2005.
24.4.2(b) Incremental		Risk assessment and treatment specifically for virtualised IT systems and services are not mentioned.

MTCS SS Level 1 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
24.4.2(c) Incremental	virtualised IT systems and services are not. Cloud Service Providers can opt to combine risk assessment and risk treatment activities for virtualised IT systems with traditional risk assessment and risk treatment activities by expanding the scope of the relevant traditional ISMS activities to include virtualisation concerns. Cloud Service Providers shall also ensure the encryption of virtual machines to protect against virtual machine theft. As an additional reference, see TR30:2012 *Technical Reference for Virtualisation security for servers* Annex A for a risk assessment worksheet on security in virtualisation.	Encryption of VMs is not mentioned is ISO/IEC 27001:2005.
24.5	**Storage area networks (SAN)**	
24.5.2(b) Incremental	ISO/IEC 27001:2005 does not cover equipment security specifically for SANs. Cloud Service Providers shall establish a process or procedure to ensure that changes to SANs and associated network components are correctly and accurately propagated.	Implementation of process for propagating all configuration changes is not mentioned.

8.2 MTCS SS Level 2

This section summarises the implementation guidelines for gaps identified between MTCS SS Level 2 and ISO/IEC 27001:2005.

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
6	**Information security management**	
6.7	**Information security liaisons (ISL)**	
6.7.3(a) New	ISO/IEC 27001:2005 does not cover the details on ISL personnel on being available for contact by customers. Cloud Service Providers shall ensure that the designated ISL personnel is available for contact by customers (e.g., cloud users).	ISO/IEC 27001:2005 Sections A.6.1.6 and A.6.1.7 mention requirement on ISL but details on being available for contact by customers are not mentioned.
6.8	**Acceptable Usage**	
6.8.3(a) Incremental	While ISO/IEC 27001:2005 covers the rules of asset acceptable usage and the information labelling, it does not include the details for the acceptable network locations. Cloud Service Providers shall make available a list of acceptable network locations for the areas mentioned in MTCS SS Clause 6.8.3(a).	Definition of rules for acceptable usage was mentioned but not details about network locations, services, devices and company-approved products.
6.8.3(b) Incremental	While ISO/IEC 27001:2005 covers information handling and network controls, it does not include the explicit authorisation process for personnel accessing customer data. Cloud Service Providers shall implement an explicit approval procedure for personnel accessing customer data via remote access technologies, or to copy, move, and store confidential data onto local hard drives and removable electronic media.	Details about handling information are mentioned in ISO/IEC 27001:2005 Section A.10.7.3 and network technologies/controls in ISO/IEC 27001:2005 Section A.11.4 but explicit authorisation or approval process was not mentioned, including access via gateways and VPNs.
7	**Human resources**	
7.1	**Background screening**	
7.1.3(a) Incremental	ISO/IEC 27001:2005 does not cover frequency of background screening. Cloud Service Providers shall conduct at least one annual background check for Personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.	Background check frequency not mentioned in ISO/IEC 27001:2005.
7.2	**Continuous personnel evaluation**	
7.2.3(a) Incremental	ISO/IEC 27001:2005 does not cover frequency of continuous personnel evaluation. Cloud Service Providers shall conduct annual evaluation for personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.	Evaluation frequency not mentioned in ISO/IEC 27001:2005.
7.2.3(b) Incremental	While ISO/IEC 27001:2005 covers the personnel evaluation, it does not include the scope of coverage of the evaluation. Cloud Service Providers shall cover at least the items as stated in MTCS SS Clause 7.2.3(b) into the personnel evaluation.	Evaluation frequency not mentioned in ISO/IEC 27001:2005.

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
7.6	**Information security training and awareness**	
7.6.3(a) Incremental	While ISO/IEC 27001:2005 covers the awareness programs in general, it does not cover the specific topic on the sensitive data in cloud environment. Cloud Service Providers shall create awareness on the importance of information security for sensitive data in the cloud environment.	Awareness in general mentioned but specific topic about sensitive data in cloud environment was not mentioned.
7.6.3(c) Incremental	While ISO/IEC 27001:2005 covers the communication of policies, it does not include the data protection policies. Cloud Service Providers shall communicate data protection policies to employees and relevant third parties.	Communication of information security policy mentioned but the communication of data protection policy though there are elements of data protection in ISO/IEC 27001:2005 Section A.15.1.4.
7.6.3(d) Incremental	While ISO/IEC 27001:2005 covers the awareness programs in general, it does not cover the specific topic on personal data. The Cloud Service Provider shall include the topic about personal data in the training and awareness programs.	Awareness in general but specific topic about personal data was not mentioned.
7.6.3(e) Incremental	While ISO/IEC 27001:2005 covers the awareness programs in general, it does not cover the specific topic on the Computer Misuse Act. Cloud Service Providers shall include the portions relevant to the information security environment and cloud computing environment of the Computer Misuse Act to the training and awareness programs.	Computer Misuse Act is not explicitly mentioned.
8	**Risk management**	
8.1	**Risk management program**	
8.1.3(a) Incremental	ISO/IEC 27001:2005 does not specify the categories of risk criteria in the risk management program. The Cloud Service Provider shall establish and document the acceptance levels into the risk management program based on risk criteria with reasonable resolution time frames and management approval. The risk criteria include, but are not limited to, the risk categories as stated in MTCS SS Clause 8.1.3(a).	Elements of risk assessment and risk acceptance are present but specific categories of risk criteria not mentioned.
8.2	**Risk assessment**	
8.2.3(a) Incremental	While ISO/IEC 27001:2005 covers the data protection requirements, it does not include them into the risk assessments. The Cloud Service Provider shall include the data protection requirements into the existing risk assessments.	Data protection elements are included in ISO/IEC 27001:2005 Section A.15.1.4 but its inclusion in risk assessment was not mentioned.
8.3	**Risk management**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
8.3.3(a) Incremental	While ISO/IEC 27001:2005 covers the prioritization of information security risks, it does not specify the prioritization of material risks. Cloud Service Providers shall evaluate and prioritise all material risks.	Priorities for managing information security risks imply prioritizing material risks.
8.3.3(d) Incremental	ISO/IEC 27001:2005 does not cover the development of a strategy for the risk remediation. Cloud Service Providers shall develop a strategy to address and mitigate identified risks.	Development of strategy not mentioned though the policy could contain specific strategies and the approach being part of a strategy.
8.4	**Risk register**	
8.4.3(a) Incremental	ISO/IEC 27001:2005 does not specify the establishment of a risk register containing the risk attributes stated in the MTSC SS Clause 8.4.3(a) in the risk management. Cloud Service Providers shall establish a risk register defining the abovementioned risk attributes in the risk management process.	Priority levels, control strategies and resolution timeframe not mentioned. Usage of a risk register was not mentioned but a risk assessment report may contain the risk register.
9	**Third party**	
9.3	**Third party agreement**	
9.3.3(a) Incremental	ISO/IEC 27001:2005 does not cover all detailed attributes as stated in MTCS SS Clause 9.3.3(a) to be addressed. Cloud Service Providers shall address the above mentioned attributes with clarity in the service level agreement with the third party service provider.	Not all detailed attributes to be addressed are present in ISO/IEC 27001:2005.
9.4	**Third party delivery management**	
9.4.3(a) Incremental	While ISO/IEC 27001:2005 covers the monitoring and review of and managing changes to third party services in general, it does not specify the implementation details with the examples as stated in the MTCS SS Clause 9.4.3(a). Cloud Service Providers shall implement the third party and sub-contracting management processes with the above mentioned examples.	Details as listed are not mentioned, but monitoring and review of third party services and monitoring of changes are mentioned in general.
9.4.3(b) Incremental	While ISO/IEC 27001:2005 covers the data protection in general, it does not specify the implementation and compliance of the data protection controls for Cloud Service Providers. Cloud Service Providers shall implement the data protection controls in accordance with regulatory requirements and ensure the compliance. In this case, as defined in the MTCS SS, a third party service provider refers to a person, organisation or entity engaged by the Cloud Service Provider that supports the cloud environment.	Mentioned in general and not specific to CSP.
10	**Legal and compliance**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
10.1	**Compliance with regulatory and contractual requirements**	
10.1.3(a) Incremental	While ISO/IEC 27001:2005 covers the review and update of the documentation, it does not specify the approach and coverage for the review and update. Cloud Service Providers shall develop an approach for the documentation review and periodical update for all categories of information system elements.	Review and update of documentations mentioned. However, there was no explicit mention of having an approach and for each category of IS element.
10.2	**Compliance with policies and standards**	
10.2.3(a) Incremental	While ISO/IEC 27001:2005 covers the review and audit for Information Security Management System in general, it does not specify the review and audit for Cloud Service Providers. Cloud Service Providers shall engage independent parties (e.g., internal audit or third party) to verify their compliance with organisational policies.	Review and audit for ISMS in general. Review and audit for CSP may include additional elements.
10.6	**Continuous compliance monitoring**	
10.6.3(a) New	ISO/IEC 27001:2005 does not cover the reporting requirements for system access. Cloud Service Providers shall implement a mechanism to provide system access reports to cloud users timely, when required.	No mention of reporting requirements on system access.
11	**Incident management**	
11.1	**Information security incident response plan and procedures**	
11.1.3(a) Incremental	While ISO/IEC 27001:2005 covers the incident response in general as part of business continuity, it does not include the designation of personnel to respond to security alerts, incident escalation procedures and customer notification procedures. Cloud Service Providers shall assign designated personnel to respond to security alerts from intrusion detection, intrusion prevention and file integrity monitoring systems in a timely manner. Cloud Service Providers shall also implement procedures for escalating incident events in order to contain and remediate the breach. In addition, Cloud Service Providers shall implement a process to notify customers and affected parties of incidents and the impact of the incidents, including the planned course of action for remediation.	Roles and responsibilities and resources mentioned but not specifically about having designated personnel available to respond to events. Consider incident response as part of business continuity.
11.1.3(d) Incremental		Incident response in general mentioned but not procedures for escalation. Consider incident response as part of business continuity.
11.1.3(e) Incremental		Notification to customers on the impact is not mentioned.
11.2	**Information security incident response plan testing and updates**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
11.2.3(a) Incremental	While ISO/IEC 27001:2005 covers the incident response in general as part of business continuity, it does not cover the requirement to maintain an up-to-date incident response plan. Cloud Service Providers shall implement a process to maintain an up-to-date information security incident response plan in accordance with industry standards.	No mention of requirement to maintain plan up to date in accordance with the industry standards. Consider incident response as part of business continuity.
11.4	**Problem management**	
11.4.3(a) Incremental	While ISO/IEC 27001:2005 covers the analysis of individual incidents and the recording of results for the actions taken to resolve the incidents, it does not specify the requirement for a trend analysis of the incidents. Cloud Service Providers shall develop a quarterly trend analysis of past incidents to identify and rectify problems.	Trend analysis was not explicitly mentioned but analysis of events and recording of results could imply a development of a similar tool.
12	**Data Governance**	
12.1	**Data classification**	
12.1.3(c) Incremental	While ISO/IEC 27001:2005 covers the classification guidelines for information, it does not specify the classification of communication channels. Cloud Service Providers shall classify communication channels to determine the sensitivity of the communication channel for secure and insecure data transmission.	Classification guidelines mentioned are for information but could possibly be applied to assets, including communication channels.
12.3	**Data integrity**	
12.3.3(b) Incremental	While ISO/IEC 27001:2005 covers message integrity, it does not specify authenticity. Cloud Service Providers shall implement controls to protect authenticity on top of message integrity.	Authenticity not mentioned explicitly but could be covered under ISO/IEC 27001:2005 Section A.12.2.2 Control of internal processing.
12.4	**Data labelling / handling**	
12.4.3(a) Incremental	While ISO/IEC 27001:2005 covers inventory of assets including media, it does not specify the requirement on the maintenance logs of all media. Cloud Service Providers shall keep maintenance logs of all media (e.g., tape drives, backup drives) in the media inventory.	Maintenance logs are not mentioned explicitly though maintenance itself is.
12.4.3(c) New	ISO/IEC 27001:2005 does not cover the requirement on the data storage location. Cloud Service Providers shall specify the location where data is stored and as per agreement with customers by Cloud Service Providers.	Requirement on location of data storage is not mentioned.
12.5	**Data protection**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
12.5.3(a) Incremental	While ISO/IEC 27001:2005 covers the information on storage, it does not include the review of the storage security. Cloud Service Providers shall conducting annual review of the security of the physical storage of media. In addition, Cloud Service Providers shall strictly prohibit distribution of any kind of media unless compelled by laws or regulations.	Storage of information is mentioned but not the review of the security of the storage.
12.5.3(b) Incremental	ISO/IEC 27001:2005 does not cover all the security mechanisms as stated in MTCS SS Clause 12.5.3(b) such as the logical access security to data and the physical access security to backup media. On top of the existing security mechanisms to monitor access the sensitive data, Cloud Service Providers shall implement the abovementioned security mechanisms.	Logical access security to data and physical access security to backup media are not mentioned.
12.5.3(c) Incremental	While ISO/IEC 27001:2005 covers the use of cryptographic controls in general, it does not specify the encryption requirements for end point devices. Cloud Service Providers shall implement strong encryption for all end point devices handling customer data.	Cryptography usage in general is mentioned but not specifically requiring having strong encryption for end point devices.
12.5.3(d) Incremental	ISO/IEC 27001:2005 does not cover the security controls for virtualised images and snapshots as stated in MTCS SS Clause 12.5.3(d). Cloud Service Providers shall implement the abovementioned security controls.	Virtualised images-specific security controls are not mentioned.
12.6	**Data retention**	
12.6.3(a) Incremental	While ISO/IEC 27001:2005 covers backup policy, it does not include the requirements on backup or redundancy mechanisms. Cloud Service Providers shall implement backup or redundancy mechanisms in accordance with legal, regulatory, and business requirements.	Backup policy is mentioned in general but not the implementation of backup or redundancy mechanisms.
12.6.3(d) Incremental	While ISO/IEC 27001:2005 requires the retention controls to be in place, it does not specify the mechanisms and rules. Cloud Service Providers shall implement periodic manual or automatic processes to identify and delete all data exceeding the retention period defined.	Brief mention of retention controls to be in place but no specific mechanism and retention rules stated.
12.9	**Secure disposal verification of live instances and backups**	
12.9.3(a) Incremental	While ISO/IEC 27001:2005 covers media disposal in general, it does not include the requirement to verify that data has been securely removed. Cloud Service Providers shall implement procedures to verify the complete removal of data from the entire cloud environment when it is deleted.	Procedure to verify that data has been securely removed is not mentioned.

MTCS SS Level 2 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
12.10	**Tracking of data**	
12.10.3(a) New	ISO/IEC 27001:2005 does not cover the requirement of the location availability of all data. Cloud Service Providers shall make available the locations of all data in production and backup environments.	Making available location information of data in production/backup environments is not mentioned.
12.11	**Production data**	
12.11.3(a) Incremental	ISO/IEC 27001:2005 does not cover the requirements to prevent migration of production data to non-production environments although it mentions segregation of environments. Cloud Service Providers shall implement the requirements as stated in MTCS SS Clause 12.11.3.	Segregation of environments is mentioned but controls to prohibit extraction/transfer of production data to non-production media is not.
12.11.3(b) Incremental		Brief mention of data duplication in a smaller context.
12.11.3(c) Incremental		Segregation of environments is mentioned but procedures for sanitization/approval before using production data in non-production environment are not.
12.11.3(d) Incremental		Establishment and communication of information security policy is mentioned. However, specific topic about copying production data into non-production environments is not mentioned.
13	**Audit logging and monitoring**	
13.1	**Logging and monitoring process**	
13.1.3(d) Incremental	While ISO/IEC 27001:2005 covers protection of logs in general, it does not specify the software to be used to prevent the changes to the logs. Cloud Service Providers shall implement file integrity monitoring or change detection software to generate alerts if there are any changes made to the logs.	Protection of logs in general, implementation of integrity monitoring or change detection software not mentioned.
13.1.3(e) New	ISO/IEC 27001:2005 does not specify the use of IDPS. Cloud Service Providers shall implement IDPS as the real time network monitoring procedures.	Intrusion Detection and Prevention Systems (IDPS) is not a requirement of ISO/IEC 27001:2005.
13.2	**Log review**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
13.2.3(a) Incremental	ISO/IEC 27001:2005 does not cover the frequency of log review. Cloud Service Providers shall conduct log review for all system components at least daily. All critical systems and servers performing security functions shall be included in the review such as intrusion detection system and authentication servers.	Periodical review is mentioned but not a specific frequency.
13.3	**Audit trails**	
13.3.3(a) Incremental	ISO/IEC 27001:2005 does not specify the media to be used for capturing audit trails. Cloud Service Providers shall write audit trails to write-only media or a tamper resistant location that prevents modifications.	Media to be used for capturing audit trails is not explicitly mentioned.
13.4	**Backup and retention of audit trails**	
13.4.3(a) Incremental	ISO/IEC 27001:2005 does not cover the backup requirements for logs. Cloud Service Providers shall ensure that only authorised personnel back up audit trails regularly to a centralised log server or media accessible.	Backing up of logs is not mentioned.
14	**Secure configuration**	
14.7	**Unnecessary service and protocols**	
14.7.3(a) Incremental	While ISO/IEC 27001:2005 covers the network security in general, it does not include the requirements on unnecessary service and protocols. Cloud Service Providers shall remove all unnecessary functionalities such as scripts, drivers, extra features, subsystems, file systems and unnecessary web servers.	Network security in general although details are not mentioned.
14.9	**Enforcement checks**	
14.9.3(a) Incremental	ISO/IEC 27001:2005 does not specify the frequency of compliance checks although technical compliance checking is covered. Cloud Service Providers shall perform checks at least weekly on security configurations.	Frequency of compliance checks is not mentioned.
14.9.3(b) New	ISO/IEC 27001:2005 does not require the implementation of file integrity monitoring tools. Cloud Service Providers shall implement file integrity monitoring tools to compare and alert unauthorised modification of critical systems, configurations and content files.	Implementation of file integrity monitoring tools is not mentioned.
15	**Security testing and monitoring**	
15.1	**Vulnerability scanning**	
15.1.3(a) Incremental	While ISO/IEC 27001:2005 requires the identification of vulnerabilities, it does not specify the mechanisms and frequency. Cloud Service Providers shall perform vulnerability scanning at least quarterly and when there are significant changes to the environment.	Identification of vulnerabilities is mentioned, but specific usage of vulnerability scanning is not. Frequency of such scans is also not mentioned.

MTCS SS Level 2 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
15.1.3(b) Incremental	While ISO/IEC 27001:2005 covers evaluation of vulnerabilities and implementation of controls in general, it does not specify the usage of the Common Vulnerability Scoring System (CVSS) to address vulnerabilities timely. Cloud Service Providers shall address vulnerabilities with a CVSS base score of 4-6.9 within one month.	Evaluation of vulnerabilities and implementation of controls to address vulnerabilities are mentioned in general. Usage of (CVSS scoring and the addressing vulnerabilities within one week are not mentioned.
16	**System acquisitions and development**	
16.1	**Development, acquisition and release management**	
16.1.3(a) New	ISO/IEC 27001:2005 does not cover the verification of the integrity and authenticity of the applications. Cloud Service Providers shall implement protection controls which allow the clients (e.g., web browsers and email clients) to verify the integrity and authenticity of the applications.	N.A
16.2	**Web application security**	
16.2.3(a) Incremental	While ISO/IEC 27001:2005 covers change control procedures, it does not cover the review of web applications using assessment tools. Cloud Service Providers shall review public-facing web applications using manual or automated application vulnerability security assessment tools or mechanisms annually or when changes are made to the applications. Tests should include identification of common web application vulnerabilities minimally.	Change control procedures are mentioned in general but not specifically the reviewing of web applications using assessment tools periodically. Minimum requirement is also not mentioned.
16.2.3(c) New	ISO/IEC 27001:2005 does not require the security testing of public web services. Cloud Service Providers shall include public web services in security testing.	N.A
16.3	**System testing**	
16.3.3(a) Incremental	ISO/IEC 27001:2005 does not include the systematic monitoring and evaluation program for all the areas as stated in MTCS SS Clause 16.3.3(a). Cloud Service Providers shall establish a systematic monitoring and evaluation program to ensure that software development is performed in accordance with industry standards and regulatory requirements. The program should cover areas as stated in MTCS SS Clause 16.3.3(a).	While some elements of a systematic monitoring and evaluation program exist, most are not mentioned (e.g., management oversight, source code review, usage of production data for test/development purposes).
16.5	**Outsourced software development**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
16.5.3(a) Incremental	While ISO/IEC 27001:2005 covers supervision and monitoring of outsourced development, it does not include the specific objective to ensure performance in accordance with industry standards and regulatory requirements. Cloud Service Providers shall establish a systematic monitoring and evaluation program to ensure that outsourced software development is performed in accordance with industry standards and regulatory requirements.	While supervision and monitoring of outsourced development is mentioned, specific objective to ensure performance in accordance with industry standards and regulatory requirements is not.
17	**Encryption**	
17.3	**Key management**	
17.3.3(a - h) Incremental	ISO/IEC 27001:2005 does not cover key management lifecycle process and controls. Refer to MTCS SS Clause 17.3.3 for specific requirements to be implemented by the Cloud Service Provider.	Specific requirement is not mentioned
18	**Physical and environmental**	
18.1	**Asset management**	
18.1.3(a) New	ISO/IEC 27001:2005 does not cover, as part of decommissioning, the control related to timely replacement of assets. The Cloud Service Provider shall perform timely replacement of assets to support the decommissioning of out-of-support systems which might be exposed to security risks.	Replacement of assets and decommissioning of out-of-support systems are not mentioned.
18.3	**Physical access**	
18.3.3(a) Incremental	ISO/IEC 27001:2005 describes generally entry controls, it does not include monitoring and storage of access logs. The Cloud Service Provider shall monitor individual access to areas hosting sensitive data and store access logs for at least three (3) months. Cloud Service Providers that adopt access card security or similar control to monitor individual access to such areas can review the access logs generated by the relevant systems.	Entry controls mentioned in general but not monitoring and storing access logs.
18.4	**Visitors**	
18.4.3(a) Incremental	ISO/IEC 2001:2005 does not include management approval as part of access control policy. The Cloud Service Provider shall establish management approval as a prerequisite before the visitors are allowed into facilities where sensitive data is hosted.	Management approval not mentioned but access control policy could include such procedures.
19	**Operations**	
19.4	**Service levels**	
19.4.3(b) Incremental	ISO/IEC 2001:2005 mandates having third party agreement, but it does not cover communication of remedies. The Cloud Service Provider shall communicate contractual remedies available to the users on failure in such third party agreements.	Contractual remedies could be included in agreements though not explicitly mentioned.

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
19.4.3(c) Incremental	ISO/IEC 2001:2005 mandates having third party agreement, but it does not include automation of alerts to the cloud user in the event of a security breach or performance degradation. The Cloud Service Provider shall include implement automated alerts to notify cloud users of potential security issues, performance degradation, and other factors that interests the cloud users.	Alerts for cloud users could be included in agreements though not explicitly mentioned.
19.6	**Recoverability**	
19.6.3(a) Incremental	ISO/IEC 2001:2005 defines controls for availability management plans but it does not cover details related to alternate sites. The Cloud Service Provider shall maintain high availability architecture of the infrastructure at the primary and alternate site.	Plans to be developed for availability mentioned, but usage of primary and alternate sites is not mentioned.
19.6.3(b) Incremental	ISO/IEC 2001:2005 defines controls related to backup management but it does not include details on adequate point-in-time backup copies. The Cloud Service Provider shall ensure availability of adequate point-in-time backup copies / snapshots of data for restoration to known consistent states.	Back-ups in general are mentioned but the requirement of having adequate point-in-time copies / snapshots is not.
20	**Change management**	
20.1	**Change management process**	
20.1.3(a) Incremental	ISO/IEC 2001:2005 does not cover the notification to cloud users in the event of changes to the systems relevant to the cloud services. The Cloud Service Provider shall establish procedures to inform affected cloud users and other third parties of such changes.	Procedures for informing affected cloud users could be included in agreements but not explicitly mentioned.
20.3	**Back-out or rollback procedures**	
20.3.3(a) Incremental	ISO/IEC 2001:2005 does not cover rollback plans and procedures as part of backup management. The Cloud Service Provider shall establish a procedure to rollback to a former version if problem is encountered during or after the deployment of changes.	Back-ups in general are mentioned. Rollback procedures could be included in agreements but not explicitly mentioned.
20.5	**Patch management procedures**	
20.5.3(a) Incremental	ISO/IEC 2001:2005 defines controls related to identification of vulnerabilities but it does not include the provision of risk ratings to vulnerabilities. The Cloud Service Provider shall identify and assign risk ratings to newly discovered security vulnerabilities.	Identification of vulnerabilities is mentioned but not the assignment of risk ratings.

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
20.5.3(b) New	ISO/IEC 2001:2005 does not cover the prioritisation and assignment of timeframes for patches. The Cloud Service Provider shall follow a risk-based approach in prioritising and defining a specific period / sequence to the application of security patches based on the level of criticality the released patch addresses.	Prioritization and definition of specific periods to application of security patches is not mentioned.
20.5.3(c) New	While ISO/IEC 2001:2005 Clause A.10.1.4 covers the separation of test and production environments, it does not specify the testing of patches. The Cloud Service Provider shall test patches in a test environment that has a setup mirroring the production environment prior to application.	ISO/IEC 27001:2005 Section A.10.1.4 covered the separation of test and production environments but testing of patches is not mentioned.
20.5.3(d) Incremental	ISO/IEC 2001:2005 does not cover hardening of dormant or offline systems. The Cloud Service Provider shall implement a process to ensure that systems that have been dormant or offline for over thirty (30) days are configured to meet hardening standards and all security software including patches is up to date. See TR 30:2012 Technical Reference for Virtualisation Security for servers Clause 8.5 Risk #4 – Security of dormant or offline VMs for additional details.	Implementation of a process to manage systems that have been dormant / offline for over 30 days is not mentioned.
22	**Cloud services administration**	
22.2	**Generation of administrator passwords**	
22.2.3(a) Incremental	ISO/IEC 2001:2005 defines controls related to good security practices for passwords but it does not include specific password criteria. The Cloud Service Provider shall implement minimum password criteria as stated in MTCS SS Clause 22.2.3(a). Alternatively, other solutions can be used where they provide equivalent or better security.	Good security practices for passwords are mentioned in general. Specific password criteria are not mentioned.
22.2.3(b) Incremental	ISO/IEC 2001:2005 does not cover two-factor authentication (2FA). The Cloud Service Provider shall implement controls such that the administrator accounts require 2FAsolution. In addition, the 2FA solution shall be implemented based on the 2FA vendor's recommended practices.	2FA is not mentioned in ISO/IEC 27001:2005.
22.2.3(c) Incremental		2FA is not mentioned in ISO/IEC 27001:2005.
22.4	**Account lockout**	
22.4.3(a) New	ISO/IEC 2001:2005 does not cover details about account lockout. The Cloud Service Provider shall ensure that accounts are locked out until another administrator unlocks it manually.	Account lockout and lockout duration are not mentioned in ISO/IEC 27001:2005.
22.5	**Password change**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
22.5.3(a) New	ISO/IEC 2001:2005 does not cover 2FA. For 2FA key or token changes, approved change management process and vendor recommended practices / configurations shall be followed.	2FA and token change procedures are not mentioned.
22.6	**Password reset and first logon**	
22.6.3(a) Incremental	ISO/IEC 2001:2005 covers generic password management but it does not cover the splitting of password. The Cloud Service Provider shall implement controls to ensure that the new password provided is split controlled and via out-of-band mechanism such that no one user has knowledge of the whole password in transit.	Password management system is mentioned in general, not specific for generation, custody and distribution of service management passwords. Split control and out-of-band mechanism are not mentioned.
22.7	**Administrator access security**	
22.7.3(a) Incremental	ISO/IEC 2001:2005 does not cover bastion hosts. Access from the network locations as stated in MTCS SS Clause 22.7.3 shall only be permitted via bastion hosts.	Bastion hosts are not mentioned.
22.8	**Administrator access logs**	
22.8.3(a) Incremental	ISO/IEC 27001:2005 covers the protection of logs in general but it does not cover controls to prevent tampering, and automatic alert or escalation of incidents concerning access control policies. The Cloud Service Provider shall implement controls as stated in MTCS SS Clause 22.8.3.	Protection of logs in general, not specifically against tampering by the administrator. Automatic alerting and escalation for violations to access control policies are also not mentioned.
22.10	**Segregation of duties**	
22.10.3(a) Incremental	ISO/IEC 27001:2005 does not define frequency of review of access rights. The Cloud Service Provider shall conduct review of access rights and segregation of duties at least on a quarterly basis	Specific frequency of review is not mentioned.
22.13	**Service and application accounts**	
22.13.3(a) Incremental	ISO/IEC 27001:2005 does not cover detailed requirements pertaining to service and application accounts. Refer to MTCS SS Clause 22.13.3 for specific requirements.	Managing and control of allocation of password in general. Implementation of either control for the creation of service accounts is not mentioned.
22.13.3(b) Incremental		Privilege management and session management in general, prohibition of caching or storing of sensitive session parameters, cookies or similar on local machines is not explicitly mentioned.

MTCS SS Level 2 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
22.13.3(c) Incremental		Privilege management and session management in general, prohibition of simultaneous logins is not explicitly mentioned.
22.13.3(d) Incremental		Privilege management in general, prohibition of console login access is not explicitly mentioned.
22.13.3(e) Incremental		Including security requirements for new systems mentioned in general, but not specifically for systems to be used in the cloud environment.
23	**Cloud user access**	
23.2	**User access security**	
23.2.3(a) New	ISO/IEC 27001:2005 does not cover two-factor authentication (2FA). The Cloud Service Provider shall implement a 2FA mechanism for users.	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
23.3	**User access password**	
23.3.3(a) Incremental	ISO/IEC 27001:2005 does not define specific criteria for passwords. The Cloud Service Provider shall implement minimum password criteria as stated in MTCS SS Clause 23.3.3(a). Alternatively, other solutions can be used where they provide equivalent or better security.	Specific password criteria are not mentioned in ISO/IEC 27001:2005.
23.4	**User account lockout**	
23.4.3(a) New	ISO/IEC 27001:2005 does not cover details pertaining to account lockout. User ID shall be locked out after a maximum of six (6) unsuccessful attempts and the lockout duration to be until an administrator enables the user ID.	Account lockout criteria are not mentioned in ISO/IEC 27001:2005.
23.4.3(b) New		Account lockout duration is not mentioned in ISO/IEC 27001:2005.
23.8	**Change of cloud user's administrator details notification**	
23.8.3(a) New	ISO/IEC 27001:2005 does not cover the alert for change in administrator details and approval being needed for changing the cloud user's administrator details. The Cloud Service Provider shall ensure that a change in the cloud user's administrator details trigger an alert to the administrator and the change shall only be effected after the Cloud Service Provider's administrator approves the change.	Alert for change in administrator details is not mentioned in ISO/IEC 27001:2005.
23.8.3(b) New		Effecting of change in administrator details is not mentioned in ISO/IEC 27001:2005.
23.10	**Communication with cloud users**	

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
23.10.3(a) Incremental	ISO/IEC 27001:2005 does not include specific topics for user education. The Cloud Service Provider shall provide user education on topics including, but not limited to, those as stated in MTCS SS Clause 23.10.3(a).	Specific topics for user education are not mentioned.
24	**Tenancy and customer isolation**	
24.2	**Supporting infrastructure segmentation**	
24.2.3(a) Incremental	ISO/IEC 27001:2005 covers network segregation but it does not include the separation of authentication sources. The authentication sources for network locations as stated in MTCS SS Clause 24.2.3(a) shall be separated.	Network segregation in general and not specific to the separation of authentication sources for cloud service components.
24.2.3(c) Incremental	ISO/IEC 27001:2005 does not include two-factor authentication (2FA). The Cloud Service Provider shall ensure that the network locations as stated in MTCS SS Clause 24.2.3(c) are segmented and no direct access is permitted, except via controlled access point with 2FA.	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
24.3	**Network protection**	
24.3.3(c) Incremental	ISO/IEC 27001:2005 does not cover the prohibition of direct public access to systems hosting sensitive data. The Cloud Service Provider shall manage and control direct public access to systems hosting sensitive data.	Prohibition of direct public access to systems hosting sensitive data not explicitly mentioned.
24.3.3(d) New	ISO/IEC 27001:2005 does not cover stateful inspection. The Cloud Service Provider shall put into place controls and configurations to implement stateful inspection.	Stateful inspection is not mentioned in ISO/IEC 27001:2005.
24.3.3(e) New	ISO/IEC 27001:2005 does not include prevention of internal IP address disclosure. The Cloud Service Provider shall put into place configurations to prevent the disclosure of internal IP address disclosure.	Internal IP address disclosure is not mentioned in ISO/IEC 27001:2005.
24.5	**Storage area networks (SAN)**	
24.5.3(c) New	ISO/IEC 27001:2005 does not cover mutual authentication between devices. The Cloud Service Provider shall leverage mutual authentication between devices on a SAN.	Mutual authentication between devices is not mentioned in ISO/IEC 27001:2005.
24.5.3(e) New	ISO/IEC 27001:2005 does not cover prevention of automatic replication. The Cloud Service Provider shall disallow automatic replication for data stored on a SAN.	Automatic replication is not mentioned in ISO/IEC 27001:2005.
24.6	**Data segregation**	
24.6.3(a) Incremental	ISO/IEC 27001:2005 does not include logical segregation for data access, logs, and encryption keys, and offsite data storage. The Cloud Service	Logical segregation for data access, logs, and encryption keys is not mentioned.

MTCS SS Level 2 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
24.6.3(b) Incremental	Provider shall ensure that logical segregation for data access, logs, and encryption keys is kept a minimum. The same segregation controls shall be applied to offsite data storage and recovery.	Security of equipment off premises in general.

8.3 MTCS SS Level 3

This section summarises the implementation guidelines for gaps identified between MTCS SS Level 3 and ISO/IEC 27001:2005.

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
7	**Human resources**	
7.1	**Background screening**	
7.1.4(a) Incremental	ISO/IEC 27001:2005 does not cover specific areas and components where background checks should be conducted. The Cloud Service Provider shall conduct at least one annual background check for all personnel. Refer to MTCS SS Clause 7.1.4(a) for examples of persons falling under this category.	Background check frequency not mentioned in ISO/IEC 27001:2005.
7.2	**Continuous personnel evaluation**	
7.2.4(a) Incremental	While ISO/IEC 27001 covers reviews in general, specific frequencies for various types of reviews are not included. The Cloud Service Provider shall ensure that annual evaluation for personnel security is conducted.	Evaluation frequency not mentioned in ISO/IEC 27001:2005.
7.3	**Employment and contract terms and conditions**	
7.3.4(a) Incremental	While acknowledgement can be implied from the signing of employment contract as covered in ISO/IEC 27001:2005, the need for re-acknowledgement is not included. The Cloud Service Provider shall require re-acknowledgement of the acceptance of Information Security Obligations Agreement from personnel at least on an annual basis and prior to the termination of service.	Implicit acknowledgement from signing of employment contract but of re-acknowledgement and re-acknowledge frequency was not mentioned.
8	**Risk management**	
8.1	**Risk management program**	
8.1.4(a) Incremental	While ISO/IEC 27001:2005 covers the evaluation of risks in general, the specific frequency for such evaluation is not included. The Cloud Service Provider shall conduct evaluation of risk components (as stated in MTCS SS Clause 8.1.4(a)) at least on a quarterly basis.	Frequency of risk review is not mentioned and risk metrics is not explicitly mentioned to be included in the scope of the review.
8.3	**Risk management**	

MTCS SS Level 3 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
8.3.4 Incremental	ISO/IEC 27001:2005 does not cover the IT risk metrics. The Cloud Service Provider shall develop a set of IT risk metrics and take into consideration components as stated in MTCS SS Clause 8.3.4(a). These IT risk metrics shall also be aligned with industry accepted risk management standards and be approved by relevant management personnel.	Metrics for the measurement of effectiveness of controls was mentioned but not metrics for IT risk.
9	**Third party**	
9.2	**Identification of risks related to third parties**	
9.2.4(a) New	While ISO/IEC 27001:2005 covers risk assessment in general, the specific need for a Threat and Vulnerability Risk Assessment (TVRA) is not included. The Cloud Service Provider shall conduct a TVRA on the third party service provider's data centre on a periodic basis by an independent third party or the cloud provider to determine the level and type of protection safeguards lacking and required, pertaining to the data centre. The scope of the TVRA should encompass the entire boundary of the in-scope service.	Risk Assessment is mentioned in general however details on TVRA at the data centre is not mentioned.
9.2.4(b) New	ISO/IEC 27001:2005 does not cover the need to have a remediation plan by third party service provider to address identified issues. The Cloud Service Provider shall ensure that the third party in question develops a remediation plan based on the TVRA that was conducted in MTCS SS Clause 9.2.24(a) and address the issues identified from the TVRA within a reasonable timeframe.	Requirement on remediation plan is included; however, specific requirement for remediation plan by third party service providers are not mentioned.
9.4	**Third party delivery management**	
9.4.4(a) New	ISO/IEC 27001:2005 does not cover specific action required from the third party service provider. The Cloud Service Provider shall ensure that a high standard of care and diligence has been performed by the third party service provider in its security policies, procedures and controls to protect the confidentiality and security of its sensitive information (categories as stated in MTCS SS Clause 9.4.4(a)).	The extent of diligence and care for the specific elements are not mentioned.
9.4.4(c) Incremental	ISO/IEC 27001:2005 does not cover the establishment of a process to monitor the performance of the third party service provider. The Cloud Service Provider shall establish a process to monitor components as stated in MTCS SS Clause 9.4.4(c). Metrics and reports provided by the third party service provider shall also be reviewed by the Cloud Service Provider.	The establishment of process to monitor third party service delivery was not mentioned.

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
9.4.4(d) Incremental	While ISO/IEC 27001:2005 covers monitoring in general, the specific need for onsite visits is not included. The Cloud Service Provider shall conduct onsite visits to the third party service provider's data centres to assess the quality of its data centre's operation and security controls. These data centres should, in the first place, be hosting sensitive data and / or applications.	ISO/IEC 27001:2005 does not mention onsite visits explicitly though monitoring is present.
9.4.4(e) Incremental	ISO/IEC 27001:2005 does not cover the establishment of disaster recovery and contingency plans and procedures by third party service provider (including components as stated in MTCS SS Clause 9.4.4(e)). The Cloud Service Provider shall ensure that the abovementioned plans and procedures have been developed by the third party service provider.	Disaster recovery and contingency planning were not mentioned.
10	**Legal and compliance**	
10.2	**Compliance with policies and standards**	
10.2.4(a) Incremental	While ISO/IEC 27001:2005 covers reviews in general, the specific frequencies for the various types of reviews are not included. The Cloud Service Provider shall conduct reviews and assessments on the third party at least on an annual basis.	Compliance or some form of alignment mentioned for ISMS policy establishment but not at the internal audit level.
10.6	**Continuous compliance monitoring**	
10.6.4(a) New	ISO/IEC 27001:2005 does not cover the provision of real-time monitoring for cloud users. The Cloud Service Provider shall have a mechanism in place to allow cloud users to monitor security of the cloud environment specific to the type of cloud services provided to these users.	No mention of security monitoring platform for cloud users.
11	**Incident management**	
11.1	**Information security incident response plan and procedures**	
11.1.4(a) Incremental	While ISO/IEC 27001:2005 Clauses A.10.6 and A.13.2 cover security measures and network controls in general, specific components as stated in MTCS SS Clause 11.1.4(a) are not included. The Cloud Service Provider shall install and configure network equipment (as stated in MTCS SS Clause 11.1.4(a)), identify and install tools as for purposes as stated in MTCS SS Clause 11.1.4(a), perform review on source code or testing on potential bottlenecks / single point of failure.	Security measures and network controls are mentioned in general, but not tools, specific network equipment or source code review.
11.1.4(b) New	ISO/IEC 27001:2005 does not cover action plans for public relations purposes. The Cloud Service Provider shall implement an action plan to address public relations issues.	N.A

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
11.1.4(c) New	ISO/IEC 27001:2005 does not cover the notification of major incidents to affected customers. The Cloud Service Provider shall implement a procedure to notify customers of major incidents and include details as stated in MTCS SS Clause 11.1.4(c) in these notifications.	Notification to customers about major security incidents is not mentioned.
11.2	**Information security incident response plan testing and updates**	
11.2.4(a) New	ISO/IEC 27001:2005 does not cover the conducting of incident drills. The Cloud Service Provider shall conduct incident drills at least twice a year with defined escalation response time and in-depth involvement and reporting from interested parties.	No mention of drills and the frequency.
12	**Data governance**	
12.4	**Data labelling / handling**	
12.4.4(a) New	ISO/IEC 27001:2005 does not cover the maintenance of logs and inventories of physical locations of cloud user data. The Cloud Service Provider shall maintain logs and inventories of physical location of all cloud users data.	Requirement on maintenance of logs and inventories of physical locations of cloud user data is not mentioned.
12.4.4(b) Incremental	While there are elements of media disposal in ISO/IEC 27001:2005 Clause 10.7, the specific requirement as stated in MTCS SS Clause 12.4.4(b) is not covered. The Cloud Service Provider shall establish and document procedures on how data is handled upon termination of the cloud service.	Documentation of such procedures is not mentioned.
12.5	**Data protection**	
12.5.4(a) Incremental	ISO/IEC 27001:2005 does not cover a data loss prevention strategy. The Cloud Service Provider shall implement a data loss prevention strategy that should address the data at the areas as stated in MTCS SS Clause 12.5.4(a).	Data validation/protection and equipment security in general mentioned no explicit mention of data loss prevention strategy.
12.6	**Data retention**	
12.6.4(a) New	ISO/IEC 27001:2005 does not cover the provision of mechanisms for cloud users to remove or destroy all data themselves. The Cloud Service Provider shall provide a mechanism to cloud users for them to remove or destroy all data, including backups, in the event of contract termination. Contract termination consists of natural expiration or premature termination.	Provision of mechanisms for cloud users to remove/destroy all data is not mentioned.
13	**Audit logging and monitoring**	
13.1	**Logging and monitoring process**	
13.1.4(d) New	ISO/IEC 27001:2005 does not cover the management of alerts. The Cloud Service Provider shall establish procedures to follow up, verify and address all alerts.	Following up, verification and addressing of alerts are not mentioned.
13.2	**Log review**	

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
13.2.4(a) New	ISO/IEC 27001:2005 does not cover the need for a tool to monitor logs on real time. The Cloud Service Provider shall implement an automated tool for real time monitoring of logs and ensure that the logs are capturing the right information necessary.	Requirement of having an automated tool for monitoring of logs is not mentioned.
14	**Secure configuration**	
14.1	**Server and network device configuration standards**	
14.1.4(a) New	ISO/IEC 27001:2005 does not cover Common Criteria EAL4. The Cloud Service Provider shall only deploy systems and infrastructure that have been certified to Common Criteria EAL4 or comparable security assurance.	No mention of compliance to Common Criteria EAL4 or similar.
14.2	**Malicious code prevention**	
14.2.4(a) Incremental	ISO/IEC 27001:2005 does not include the testing of prevention and detection capabilities present in the cloud infrastructure. The Cloud Service Provider shall conduct periodic testing of the prevention and detection capabilities and recovery procedures of the cloud infrastructure against malicious code.	Controls against malicious codes are mentioned but periodic testing is not mentioned.
14.2.4(b) Incremental	ISO/IEC 27001:2005 does not cover the sandboxing or isolation of any user provided code. The Cloud Service Provider shall ensure that any user provided code is sandboxed or isolated to ensure the underlying platform and other tenants are not affected by the change.	Controls against malicious codes are mentioned but specific control requirements are not mentioned.
14.9	**Enforcement checks**	
14.9.4(a) Incremental	While ISO/IEC 27001:2005 covers technical compliance checks, the specific frequency for such checks are not mentioned. The Cloud Service Provider shall ensure that enforcement checks are performed at least on a daily basis for security configurations.	Frequency of compliance checks is not mentioned.
14.9.4(b) New	ISO/IEC 27001:2005 does not cover file integrity monitoring tools. The Cloud Service Provider shall implement file integrity monitoring tools to compare and alert immediately on occasions as stated in MTCS SS Clause 14.9.4(b).	Implementation of file integrity monitoring tools is not mentioned.
15	**Security testing and monitoring**	
15.1	**Vulnerability scanning**	
15.1.4(a) Incremental	ISO/IEC 27001:2005 does not cover details of vulnerability (both internal and external) scanning as stated in MTCS SS Clause 15.1.4. Vulnerability scanning, both internal and external, shall be performed at least on a monthly basis. Cloud Service Providers can use vulnerability scanning as a check to ensure patching is performed based on MTCS SS Clause 20.5.4(a).	Identification of vulnerabilities is mentioned, but specific usage of vulnerability scanning is not. Frequency of such scans is also not mentioned.

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
15.2	**Penetration testing**	
15.2.4(a) New	ISO/IEC 27001:2005 does not specifically cover penetration testing. Cloud Service Providers shall conduct penetration testing at least twice annually, with at least one of the tests performed by a qualified third party.	Penetration testing is not mentioned in ISO/IEC 27001:2005.
15.3	**Security monitoring**	
15.3.4(a) Incremental	While elements of monitoring are present in ISO/IEC 27001:2005, details pertaining to the depth and scope of the reviews are not included. The Cloud Service Provider shall include the requirements as stated in MTCS SS Clause 15.3.4(a) in its security monitoring process.	Identification and establishment of depth and scope of compliance review not mentioned. Assessing technical competencies not explicitly mentioned though ISO/IEC 27001:2005 Section 5.2.2 could lead to the technical assessment of the personnel.
16	**System acquisitions and development**	
16.1	**Development, acquisition and release management**	
16.1.4(a) New	ISO/IEC 27001:2005 does not cover the review of custom code. The Cloud Service Provider shall perform regular reviews of custom code prior to release to production to identify any potential vulnerabilities in the code. These reviews shall be conducted by parties as stated in 16.1.4(a).	N.A
16.2	**Web application security**	
16.2.4(a) New	ISO/IEC 27001:2005 does not cover web application testing. The Cloud Service Provider shall conduct web application testing and ensure that private / protected web services interfaces are included in the scope of tests.	N.A
17	**Encryption**	
17.3	**Key management**	
17.3.4(a) Incremental	ISO/IEC 27001:2005 does not cover the storage of encryption keys. The Cloud Service Provider shall ensure that encryption keys are stored in tamper-resistant device.	Specific requirement is not mentioned.
19	**Operations**	
19.2	**Documentation of service operations and external dependencies**	
19.2.4(a) Incremental	ISO/IEC 27001:2005 does not cover cloud specific documentations. The Cloud Service Provider shall include in its documentation, all external dependencies in providing the cloud services.	External dependencies not explicitly mentioned for documentation.
19.3	**Capacity management**	

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
19.3.4(a) New	ISO/IEC 27001:2005 does not cover tools for capacity monitoring. The Cloud Service Provider shall put in place automated monitoring tools to continually monitor critical resources for capacity utilisation (components as stated in MTCS SS Clause 19.3.4(a)) and ensure that alert notification types and rules are appropriately set.	Usage of tools for monitoring critical resources for capacity utilisation is not mentioned.
19.4	**Service levels**	
19.4.4(a) Incremental	ISO/IEC 27001:2005 does not cover service levels and performance in the contractual agreements and other means of communication acceptable to the cloud users. The Cloud Service Providers shall fulfil requirements listed in MTCS SS Clause 19.4.4 on top of ISO/IEC 27001:2005 Clauses A.6.2 and A.10.2: • communication of the details on redundant network connectivity links to the cloud users • communication of the minimum bandwidth available to the cloud users • communication of the protection measures available against malicious attacks to the cloud users • communication of the quality of service (QoS) controls available to the cloud users • communication of the bandwidth scalability on storage links to the cloud users • communication of any known limitation on the application / service to the cloud users	Redundant network connectivity links could be included in agreements though not explicitly mentioned.
19.4.4(b) Incremental		Communication of minimum bandwidth available to users could be included in agreements though not explicitly mentioned.
19.4.4(c) Incremental		Communication of available protection measures against malicious attacks could be included in agreements though not explicitly mentioned.
19.4.4(d) Incremental		Communication of QoS controls could be included in agreements though not explicitly mentioned.
19.4.4(e) Incremental		Bandwidth scalability could be included in agreements though not explicitly mentioned.
19.4.4(f) Incremental		Limitations could be included in agreements though not explicitly mentioned.
19.5	**Reliability and resiliency**	
19.5.4(a) Incremental	ISO/IEC 27001:2005 does not cover reliability and resiliency of storage systems. The Cloud Service Providers shall fulfil specific requirements listed in MTCS SS Clause 19.5.4 to enhance storage, network security management, backup and information security components.	Review of ISMS and BCP in general, specific coverage of review is not mentioned.
19.5.4(b) New		Resiliency for storage systems is not mentioned.
19.5.4(c) New		Redundancy for SANs is not mentioned.
19.5.4(d) Incremental		Management and control of networks mentioned in general but not specific network equipment and components.

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
19.5.4(e) Incremental		Management and control of networks mentioned in general but not specifically availability for network equipment and components.
19.5.4(f) Incremental		Back-ups in general, specific use of mirrored or RAID not mentioned.
19.5.4(g) New		While back-up is covered generally under A10.5.1, hot spares are not.
19.5.4(h) Incremental		Implementation of capabilities specific for the detection of outages of storage systems is not mentioned.
20	**Change management**	
20.3	**Back-out or rollback procedures**	
20.3.4(a) Incremental	ISO/IEC 27001:2005 does not cover alternate recovery options. The Cloud Service Provider shall explore alternate recovery options if the any change applied is not successfully implemented in the production environment and cannot be roll backed to a former version.	Back-ups in general are mentioned. Alternate recovery options could be included in agreements but not explicitly mentioned.
20.5	**Patch management procedures**	
20.5.4(a) New	ISO/IEC 27001:2005 does not cover patch management procedures. The Cloud Service Provider shall establish procedures to justify and track to closure patches that are not applied.	Patch management procedures are not mentioned.
21	**Business continuity planning (BCP) and disaster recovery (DR)**	
21.2	**BCP and DR plans**	
21.2.4(a) Incremental	ISO/IEC 27001:2005 does not cover rapid operational and backup capabilities. The Cloud Service Provider shall implement rapid operational and backup capabilities at the individual system / application cluster level.	Implementation of rapid operational and backup capabilities is not mentioned.
21.2.4(d) Incremental	ISO/IEC 27001:2005 does not cover alternate recovery site. The Cloud Service Provider shall set up an alternate recovery site geographically separated from the primary site to enable restoration / resumption of critical systems and business operations.	Set up of alternate recovery site is not mentioned.
21.3	**BCP and DR testing**	

MTCS SS Level 3 clause	**Implementation guidance**	**Additional context on gaps identified on ISO/IEC 27001:2005**
21.3.4(a) Incremental	ISO/IEC 27001:2005 does not cover disaster recovery components. Cloud Service Providers shall ensure that business continuity and disaster recovery plans are tested and updated at least on an annual basis, and include plans for various test case scenarios (refer to MTCS SS Clause 21.3.4(a) for examples).	Disaster recovery is not mentioned in ISO/IEC 27001:2005 though elements of it can be found in business continuity planning-related clauses. Specific frequency for testing is not mentioned. Specific test case scenarios are also not mentioned.
22	**Cloud services administration**	
22.6	**Password reset and first logon**	
22.6.4(a) Incremental	ISO/IEC 27001:2005 does not cover details on password reset and change. The Cloud Service Provider shall implement appropriate mechanism such that half of the new password is provided via an out-of-band mechanism directly to the affected person and the other half is provided to their supervisor.	Password management system is mentioned in general, the need for having two halves of a password, with each half given to different person, is not mentioned.
22.7	**Administrator access security**	
22.7.4(a) Incremental	ISO/IEC 27001:2005 does not cover privilege access management tools. The Cloud Service Provider shall implement privilege access management tools to restrict administrators' direct access to privileged functions and accounts.	Control of access in accordance with the defined access control policy in general. Usage of privilege access management tools is not mentioned.
22.1	**Segregation of duties**	
22.10.4(a) Incremental	While ISO/IEC 27001:2005 covers the review of user access rights and the segregation of duties, the specific frequency of such reviews is not included. The Cloud Service Provider shall conduct access rights and segregation of duties review at least on a monthly basis.	Specific frequency of review is not mentioned.
22.12	**Third party administrative access**	
22.12.4(a) Incremental	ISO/IEC 27001:2005 does not cover the granting of access to vendors. The Cloud Service Provider shall only allow third party access to the environment under the direct supervision of the Cloud Service Provider's relevant personnel.	Requirement of direct supervision by CSP's relevant personnel is not mentioned.
22.13	**Service and application accounts**	
22.13.4(a) Incremental	ISO/IEC 27001:2005 does not cover service and application accounts. The Cloud Service Provider shall establish procedures to change service account passwords at least twice annually or when an administrator leaves the organisation.	Procedures and frequency for change of service account passwords are not mentioned.
23	**Cloud user access**	
23.2	**User access security**	

MTCS SS Level 3 clause	Implementation guidance	Additional context on gaps identified on ISO/IEC 27001:2005
23.2.4(a) New	ISO/IEC 27001:2005 does not cover identity management. The Cloud Service Provider shall utilise federated identity management to coordinate authentication and authorisation with enterprise or third party systems, and avoid storing same user identity in multiple cloud environments.	Identity management is not mentioned in ISO/IEC 27001:2005.
24	**Tenancy and customer isolation**	
24.1	**Multi tenancy**	
24.1.4(a) New	ISO/IEC 27001:2005 does not cover multi tenancy and segregation between virtual machines belonging to different users not mentioned in ISO/IEC 27001:2005. The Cloud Service Provider shall implement monitoring mechanisms to detect if one virtual host attempts to access another virtual host. Cloud Service Providers shall also ensure that virtual hosts with different security profiles are not hosted on the same system. Security profiles refer to each organisation's user access control matrix (i.e. super user, administrator, business user). In addition, communication between virtual hosts that is going outside of each cloud user's environment shall pass through a firewall (or equivalent) shall be configured to only allow the minimum traffic necessary for the function.	Implementation of monitoring mechanisms to detect the specified requirement is not mentioned.
24.1.4(b) New		Virtual hosts are not mentioned in ISO/IEC 27001:2005.
24.1.4(c) New		Virtual hosts are not mentioned in ISO/IEC 27001:2005.
24.5	**Storage area networks (SANs)**	
24.5.4(a) New	ISO/IEC 27001:2005 does not cover equipment security for SANs. The Cloud Service Provider shall leverage hard zones configured in the FC switch or similar controls. Where feasible, leverage Logical Unit Numbers (LUN) masking or similar controls on storage devices. Cloud Service Providers should also provide options for customers to maintain control of the encryption keys.	Hard zones are not mentioned in ISO/IEC 27001:2005.
24.5.4(b) New		(LUN masking is not mentioned in ISO/IEC 27001:2005.
24.5.4(d) New		Option for customers to maintain control of the encryption keys is not mentioned.
24.6	**Data segregation**	
24.6.4(a) Incremental	ISO/IEC 27001:2005 does not cover cloud user control over encryption keys. The Cloud Service Provider shall ensure that encryption keys can be controlled by the cloud user.	Allowing cloud user control of encryption is not mentioned.
24.6.4(b) New	ISO/IEC 27001:2005 does not include logical segregation for backups. The Cloud Service Provider shall ensure that backups are segregated by user.	Segregation of back-ups by users is not mentioned in ISO/IEC 27001:2005.

<End of Implementation Guideline Report>