INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS) Audit Checklist Report

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

December 2014

Revision History

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

Disclaimer

The information provided in this Audit Checklist Report is for general information purposes only. The Audit Checklist 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 Audit Checklist Report. The Working Group and IDA are entitled to add, delete or change any information in the Audit Checklist 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 feedbacks 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 Audit Checklist Report is the third 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.

This Audit Checklist Report and associated audit procedures are intended to help ISO/IEC 27001:2005 certified Cloud Service Providers carry out trial cross-certification with auditors / Certification Bodies for MTCS SS. As such, this document does not include audit related information on recommended audit timeline and competency criteria for auditors.

Note that this report only covers gaps identified in Gap Analysis Report. It is recommended for Cloud Service Providers and auditors to view the complete set of audit procedures listed in the MTCS SS document.

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 the 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 the 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 the MTCS SS certification audit when the scope of ISO/IEC 27001:2005 audit overlaps with scope of the MTCS SS audit.

3 Intended Audience

This Audit Checklist 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 required audit procedures.

4 Scope

This report only covers gaps identified between ISO/IEC 27001:2005 and MTCS SS as listed in the Gap Analysis Report. The main goal of the listed audit procedures is to aid Cloud Service Providers to cross certify from ISO/IEC 27001:2005 to MTCS SS.

The Audit Checklist Report includes the gaps identified in Gap Analysis Report, which are classified as "INCREMENTAL" or "NEW". Note that requirements that were listed as "INCLUDED" in the Gap Analysis Report will not be discussed in this document.

5 Document Structure

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

- Section 6 – Terms and Definitions
- Section 7 – Tips on Using this Audit Checklist Report
- Section 8 – Audit Checklist

6 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.

7 Tips on Using this Audit Checklist Report

Section 8 includes the corresponding audit procedures required for gaps identified in Gap Analysis Report. This list is intended to guide auditors and ISO/IEC 27001:2005 certified Cloud Service Providers in auditing and adopting MTCS SS Levels 1, 2 or 3. From the Cloud Service Providers' perspective, this document serves as a general guide for providers to understand the incremental scope covered in MTCS SS certification audits when they are already ISO/IEC 27001:2005 certified.

Cloud Service Providers should refer to the audit checklist listed for the targeted and preceding Level if they are looking to be certified in MTCS 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 the audit checklist 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'. The concept above also applies to auditors, including internal audit function and MTCS SS external auditors.

It is recommended for Cloud Service Providers to refer to the Implementation Guideline Report while using this document. It is also recommended for Cloud Service Providers and auditors to view the complete set of audit procedures listed in the MTCS SS document for the authoritative list of requirements and audit procedures.

Descriptions of the respective columns for the checklists in Sections 8.1, 8.2 and 8.3 are listed below:

Note that a "√" in the respective columns indicates whether the control requires document review, system review or visual inspection recommended as part of the audit activities to be performed by the assessors

Column	Column description
Organisational Control	Auditors shall gather evidence of the performance of organisational controls through review of the records of performance of controls, interviews and observations. Main questions to answer are: 1. Does the organisation have documented controls? 2. Is the role and responsibility clear and complete?
Technical Control / System Review	Auditors shall gather evidence on the performance of technical / physical controls through system review, which can be performed via a set of technical activities. Examples of these technical activities include, but are not limited to the following: 1. Inspection of system, or device configurations / settings 2. Physical inspection of controls Main questions to answer are: 1. Are controls implemented as documented? 2. Do controls meet MTCS requirements?
Effectiveness Review (Note: For MTCS SS Level 3 control and audit procedure, a higher level of requirement is needed. Auditors conducting MTCS SS Level 3 certifications should rely on this audit activity when possible)	Auditors shall visually inspect controls on site or at the location to evaluate their effectiveness. This means that it is not sufficient to review the respective documentation on paper or through interviews – the auditors need to verify the controls at the location (if necessary) where it is implemented. Evaluation and review of testing results produced from previous tests performed by personnel from the Cloud Service Provider or third-parties engaged by the Cloud Service Provider. Main questions to answer are: 1. Are the controls implementation effective to the risk level? 2. Do controls implemented achieve their purpose?

While selecting and deciding on the audit activities to be performed, Auditors / Certification Bodies shall take into consideration the impact of non-compliance to the Cloud Service Provider's operations, the importance of the specific security control specified in MTCS SS and the cost of performing the audit activity. From this point of view, the audit activities for cross-certification with MTCS SS Level 3 are more demanding relative to MTCS SS Levels 2 and 1.

8 Audit Checklist

8.1 MTCS SS Level 1

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

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6		**Information security management**			
6.1		**Information security management system (ISMS)**			
6.1.2(e) Incremental 6.1.2(i)-(j) Incremental	6.1.2 (a)	ISO/IEC 27001:2005 does not cover specific details related to risk mitigation. Determine if the technical and / or procedural controls, associated with the following have been implemented in the ISMS: • mitigate risk from authorised insiders, • mitigate risk associated with cloud computing; and • manage virtualisation security for cloud services.	√	√	
6.4		**Information security policy**			
6.4.2(b) Incremental	6.4.2(b)-(c)	ISO/IEC 27001:2005 does not cover all aspects of the development of a strategic plan. Determine if an appropriate strategic plan and security program with sufficient details on roles and responsibilities is in place. The information security policy should mandate management commitment and define the approach to manage information security.	√		
6.6		**Information security audits**			
6.6.2(a) Incremental	6.6.2(a)	ISO/IEC 27001:2005 does not cover the establishment of an audit committee. Determine if an audit committee has been established and covers the appropriate information security areas as defined in MTCS SS Audit Procedure 6.6.2(a).	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6.6.2(b) Incremental	6.6.2(b)	ISO/IEC 27001:2005 does not cover the approval of IT security audit plans by a formal audit committee. Determine if IT security audit plans have been approved by the audit committee formed in MTCS SS Requirement 6.6.2(a).	√		
6.6.2(c) Incremental	6.6.2(c)	ISO/IEC 27001:2005 does not specify the frequency for conducting IT security audits. Review relevant documents or reports to verify that security audits have been conducted at least on an annual basis.	√		
6.7		**Information security liaisons (ISL)**			
6.7.2(d) Incremental	6.7.2(b)	ISO/IEC 27001:2005 does not cover the inclusion of external risk development as part of the internal awareness program. Verify that knowledge of external risk development has been included as one of the topics for awareness and training.	√		
6.8		**Acceptable Usage**			
6.8.2(a) Incremental 6.8.2(b) Incremental	6.8.2(c)	ISO/IEC 27001:2005 does not cover details on approval procedures and rules for acceptable usage for authentication technology, service, device or company-approved product (e.g., user ID, password, token). Verify that appropriate approval procedures are in place for the authorisation of use of authentication technology, service, device or company-approved product by authorised parties.	√		
7		**Human resources**			
7.1		**Background screening**			
7.1.2(b) Incremental	7.1.2(c)	Determine if background checks for personnel have been conducted in sufficient detail and covered appropriate areas as stated in MTCS SS Requirement 7.1.2(b) commensurate with the person's roles and responsibilities.	√		
8		**Risk management**			
8.2		**Risk assessment**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
8.2.2(a)-(c) Incremental	8.2.2(a)-(c)	ISO/IEC 27001:2005 does not cover cloud specific areas in the general ISMS risk assessment. Verify that risk assessments have been conducted at least on an annual basis, or when there is significant change on any organisational control (e.g., security policies, procedures, standards), or system components relevant to the operation of the cloud services. Verify that the risk assessments are conducted in sufficient detail and cover the activities as stated in MTCS SS Requirement 8.2.2(a), risk categories as stated in MTCS SS Requirement 8.2.2(b), and include the likelihood and impact of all inherent and residual risks identified in MTCS SS Requirement 8.2.2(c).	√		
9		**Third party**			
9.1		**Third party due diligence**			
9.1.2(a) Incremental	9.1.2(a)	ISO/IEC 27001:2005 does not cover specific criteria for third party due diligence (e.g., viability, capability, track record). Determine if risks as stated in MTCS SS Clause 9.1.1 have been understood and addressed. Determine if sufficient due diligence (with components as stated in MTCS SS Requirement 9.1.2(a)) were carried out before engaging a third party service provider.	√		
9.4		**Third party delivery management**			
9.4.2(c) New	9.4.2(c)	ISO/IEC 27001:2005 does not cover the implementation of security policies, procedures and controls by third party service providers. Determine if the cloud service provider has a process to review if security policies, procedures and controls implemented by third party service providers are at least as stringent as their own.	√		√

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
10		**Legal and compliance**			
10.1		**Compliance with regulatory and contractual requirements**			
10.1.2(b) New 10.1.2(d) New	10.1.2(b)	ISO/IEC 27001:2005 does not cover cloud specific requirements regarding cross-border movement and data. Determine if cross-border and data transit requirements (e.g., location of data hosting, differing regulation in hosting and user countries, international standards) have been taken into consideration and are maintained by the Cloud Service Provider.	√		
10.2		**Compliance with policies and standards**			
10.2.2(a) Incremental	10.2.2(a)-(b)	ISO/IEC 27001:2005 does not cover cloud specific requirements regarding review and audit activities. Determine if the following controls have been implemented: • Independent (i.e., internal audit or third party) reviews and assessments have been performed for policies and standards that have bearing on the relevant cloud services. • Reviews were performed at planned intervals, or when there are significant changes to the cloud environment. • All relevant cloud services comply with the organisational policies and standards including those stated in MTCS SS Clause 10.2.1.	√		
10.3		**Prevention of misuse of cloud facilities**			
10.3.2(a)-(b) Incremental	10.3.2(a)	ISO/IEC 27001:2005 does not specifically cover prevention of misuse of cloud facilities.	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
10.3.2(c)-(d) New		Determine if the following controls have been implemented: • employees and third parties are aware of the scope of permitted access and use of the cloud environment, • training sessions pertaining to the monitoring policies, procedures and tools in place have been conducted, • configuration of log-on warning messages or reminder on access policies, • monitoring for accessing infrastructure or other privileged access; and • monitoring for detecting if the cloud infrastructure is being used as a platform to attack others.			
10.4		**Use of compliant cryptography controls**			
10.4.2(c) New	10.4.2(a)	ISO/IEC 27001:2005 does not cover the knowledge of and application of prevailing industry practices in the usage of cryptographic controls. Determine if the Cloud Service Provider has knowledge of and is applying prevailing industry practices in the usage of cryptographic controls.	√	√	
10.6		**Continuous compliance monitoring**			
10.6.2(a) Incremental	10.6.2(a)	ISO/IEC 27001:2005 does not cover the provision of continuous or real-time compliance monitoring. Verify if a system configuration compliance reporting framework for critical data separation and access against deployed configuration baselines and access matrices, which include	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
10.6.2(b) Incremental		those as stated in MTCS SS Requirement 10.6.2(a), has been implemented. Verify if a process or system for cloud users to monitor event logs has been implemented based on the suggested implementation guidelines or the implementation of equivalent controls.			
11		**Incident management**			
11.1		**Information security incident response plan and procedures**			
11.1.2(a) Incremental 11.1.2(b) Incremental 11.1.2(c) New 11.1.2(e) Incremental 11.1.2(g) Incremental	11.1.2(a)-(c)	ISO/IEC 27001:2005 does not cover all of the elements required by MTCS SS for an incident response plan and procedures. Determine if the following have been defined in the incident response plan: • roles and responsibilities for Cloud Service Provider and relevant parties supporting or providing cloud services, • internal and external communication and contact procedures, • information security incident response, escalation and recovery procedures together with resolution time frames, • extent of cooperation among Cloud Service Provider and relevant parties supporting or providing cloud services has been specified in a Service Level Agreement (SLA), • classification and prioritisation of incidents by potential	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
11.1.2(h) Incremental 11.1.2(i) Incremental		severity levels (if content is part of the incident response plan), • appropriate method of notification to notify affected customers within reasonable time after detection of security breach; and • provision of capability to provide cloud users with required digital forensic evidence.			
11.2		**Information security incident response plan testing and updates**			
11.2.2(a) Incremental 11.2.2(b) New 11.2.2(c) Incremental	11.2.2(a)-(b)	ISO/IEC 27001:2005 does not cover the testing and updates of incident response plan. Determine if types of tests, test scope and parties to be involved in the test execution and review have been included in an incident response test plan, verify that the information security incident response plan is tested on an annual basis and determine if appropriate training has been given to personnel assigned with information security incident plan.	√	√	√
11.3		**Information security incident reporting**			
11.3.2(b) Incremental	11.3.2(b)	ISO/IEC 27001:2005 does not cover the notification and provision of support to the relevant cloud users and third parties affected during a security breach. Determine if a well-defined process exists to notify and support relevant cloud users and third parties affected by the security breach of information systems and services in a timely manner.	√		
11.4		**Problem management**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
11.4.2(c) Incremental	11.4.2(c)	ISO/IEC 27001:2005 does not cover the establishment of escalation processes for problems with different severity levels. Determine if there are clear processes and procedures for the escalation of problems with different severity levels based on the suggested implementation guidelines or the implementation of equivalent controls. Also, verify that relevant management approvals have been obtained for the escalation processes and procedures.	√		
12		**Data Governance**			
12.5		**Data protection**			
12.5.2(a) Incremental	12.5.2(a)	ISO/IEC 27001:2005 does not cover specific media handling processes for virtualised images and snapshots. Determine if sufficient security controls have been implemented over access to all media, virtualised images and snapshots to protect data from loss and destruction.	√	√	
12.7		**Data backups**			
12.7.2(b) Incremental	12.7.2(b)	ISO/IEC 27001:2005 does not cover the frequency of testing required on the backups. Determine if an appropriate frequency of testing on backups has been defined and implemented.	√		
12.7.2(c) Incremental	12.7.2(d)	ISO/IEC 27001:2005 does not cover the access and storage locations of the backups. Determine if appropriate access and storage locations for backups have been defined and if security controls in place are sufficient.	√	√	
12.8		**Secure disposal and decommissioning of hardcopy, media and equipment**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.8.2(c) New	12.8.2(c)-(d)	Secure disposal and decommissioning procedures of hardcopy materials are not mentioned in ISO/IEC 27001:2005. Determine if hardcopy materials have been appropriately destroyed (via methods mentioned in MTCS SS Requirement 12.8.2(c)) or if a "Certificate of Destruction" has been obtained from a data disposal third party upon destruction of these hardcopy materials. Inspect the shredding facility to determine the appropriateness of the controls.	√	√	
13		**Audit logging and monitoring**			
13.1		**Logging and monitoring process**			
13.1.2(f) Incremental	13.1.2(d)	ISO/IEC 27001:2005 does not cover audit logging and log review. Verify if reviews have been done for the logging of identification and authentication mechanism usage, and audit trail files initialisation, and ensure that reviews on identification and authentication are conducted based on management-approved settings and configuration documents.	√	√	
13.3		**Audit trails**			
13.3.2(a) Incremental	13.3.2(a)	ISO/IEC 27001:2005 does not cover the level of details to be included in audit trails. Determine if audit trails contain an appropriate level of details for underlying events as stated in MTCS SS Requirement 13.3.2(a).		√	
13.5		**Usage logs**			
13.5.2(a) Incremental	13.5.2(a)-(c)	ISO/IEC 27001:2005 does not cover the protection of strict files and directories' permissions of usage logs. Verify that the following criteria of the usage logs are in place: • Usage logs cannot be modified. • Strict files and directories' permissions have been set on the storage location storing the usage logs.		√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14		**Secure configuration**			
14.1		**Server and network device configuration standards**			
14.1.2(a)-(e) Incremental	14.1.2(a)-(c)	ISO/IEC 27001:2005 does not cover the detailed components of the network security management controls, and system hardening standards. Determine if controls related to MTCS SS Requirement 14.1.2 regarding server and network device configuration standards have been implemented.	√	√	
14.2		**Malicious code prevention**			
14.2.2(b)-(g) Incremental	14.2.2(b)-(g)	ISO/IEC 27001:2005 does not cover specific control requirements for malicious code prevention. Refer to MTCS SS Audit Procedures 14.2.2(b)-(g) for specific audit procedures regarding malicious code prevention. Determine if appropriate awareness procedures pertaining to malicious code prevention have been given to administrators of cloud systems.	√	√	
14.4		**Physical port protection**			
14.4.2(b)-(c) Incremental	14.4.2(a)-(b)	ISO/IEC 27001:2005 does not specifically cover physical port protection on top of the network access controls network access controls. Verify that all unused physical and / or logical ports have been disabled / removed, and configurations required for hardening have been implemented.		√	
14.7		**Unnecessary service and protocols**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14.7.2(a)-(c) Incremental	14.7.2(a)-(c)	ISO/IEC 27001:2005 does not cover the detailed characteristics specified in MTCS SS Clause 14.7.2(a)-(c) to prevent the misuse of services and protocols. Conduct system configuration reviews to verify that only necessary and secure services, protocols and daemons required for the functioning of the system have been enabled. Also, determine if any insecure features necessary for required services is enabled.		√	
15		**Security testing and monitoring**			
15.1		**Vulnerability scanning**			
15.1.2(a) Incremental	15.1.2(a)	ISO/IEC 27001:2005 does not cover vulnerability scannings. Determine if internal and external vulnerability scans, as specified in MTCS SS Audit Procedure 15.1.2(a), have been conducted at least on a quarterly basis by reviewing assessment reports and scan results.	√		
15.1.2(b) Incremental	15.1.2(b)	ISO/IEC 27001:2005 does not cover vulnerability scannings. Review a sample of scan results and verify that vulnerabilities identified with a CVSS score of 7 – 10 were addressed within a week of detection of the vulnerability, as specified in MTCS SS Audit Procedure 15.1.2(b).		√	
15.2		**Penetration testing**			
15.2.2(a) New	15.2.2(a)	ISO/IEC 27001:2005 does not specifically require penetration testing. Verify that internal and external penetration testing from locations as stated in MTCS SS Clause 15.2.1 was conducted at least on an annual basis.	√		
15.3		**Security monitoring**			
15.3.2(b) New	15.3.2(b)	Verify that intrusion detection systems, and / or intrusion prevention systems to monitor traffic within the cloud environment have been implemented, as specified in MTCS SS Audit Procedure 15.3.2(b).		√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
15.3.2(c) Incremental	15.3.2(c)	Determine if policies on security principles for network intrusion, detection and prevention have been established and are up-to-date.	√		
16		**System acquisitions and development**			
16.1		**Development, acquisition and release management**			
16.1.2(a)-(d) Incremental	16.1.2(a)-(g)	ISO/IEC 27001:2005 does not cover all of MTCS SS Clause 16.1.2(a)-(d) and MTCS SS Clause 16.1.2(j)-(l) regarding the policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities. Determine if the following controls are in place: • Software applications have been developed in accordance with industry accepted practices and incorporate information security throughout the software development life cycle. • Custom application accounts, user IDs, and passwords have been removed before applications become active	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
16.1.2(j)-(l) New		or are released to customers. • Test data and accounts have been removed before production systems become active. • Prevent common coding vulnerabilities in software development processes by verifying the applications against industry standards. • Static code analysis tools have been used against all source code. • Data validation has been performed and protection controls have been developed in the application. • Source-code has been established as being authentic. • Programs are free of spyware, trojans, backdoors, logic bombs and other non-authorised sub-routines.			
16.4		**Source code security**			
16.4.2(a) Incremental	16.4.2(a)-(b)	ISO/IEC 27001:2005 does not cover version control. Review the access to the source code repository to ensure that only authorised personnel have been granted access. In addition, verify that version control is followed.		√	
17		**Encryption**			
17.1		**Encryption policies and procedures**			
17.1.2(a)-(b) Incremental	17.1.2(a)-(c)	Verify that encryption policies and procedures have been appropriately documented for the requirements as stated in MTCS SS Requirement 17.1.2(a). Verify that encryption policies have been applied to sensitive information in-transit and in-storage. Verify if the policies and procedures have been periodically reviewed, updated and approved by the management.	√		
17.2		**Channel encryption**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
17.2.2(a) Incremental	17.2.2(a)	ISO/IEC 27001:2005 does not cover specific usage of encryption. Inspect if sensitive data transmissions, non-console administrative access and all electronic commerce transactions have been protected by applicable cryptographic methods, as stated in MTCS SS Audit Procedure 17.2.2(a).		√	
17.3		**Key management**			
17.3.2(a)-(d) Incremental	17.3.2(a)-(e)	As outlined in MTCS SS Audit Procedures 17.3.2(a)-(e), verify that appropriate procedures have been implemented for secure cryptographic storage, distribution and change, and if formal acknowledgement of responsibilities from key custodians has been obtained.	√		
17.4		**Electronic messaging security**			
17.4.2(b) Incremental 17.4.2(c) New 17.4.2(d) Incremental 17.4.2(e) New 17.4.2(f) Incremental	17.4.2(b)-(d)	ISO/IEC 27001:2005 does not cover the details on electronic messaging security as stated in MTCS SS Clause s 17.4.2(b)-(f). Determine if the following controls are in place: • Correct addressing and transportation of information involved in electronic messaging. • Use of less-secure messaging systems have been limited, controlled or blocked. • Stronger levels of authentication and message content protection have been implemented when using public networks. • Use of appropriate open standards (e.g., Sender Policy Framework or DomainKey (DKIM)) to prevent and detect spoof emails. • Implementation of digital signatures on emails to secure email communications between the Cloud Service Providers and cloud users.	√	√	
18		**Physical and environmental**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
18.1		**Asset management**			
18.1.2(c) Incremental	18.1.2(c)	ISO/IEC 27001:2005 does not cover the need to protect equipment supporting sensitive / critical applications. Determine if an appropriate procedure is in place to ensure all equipment supporting sensitive / critical applications or data are correctly maintained, protected from power failures and have applicable redundancies based on risk of failure.	√	√	
18.1.2(d) New	18.1.2(d)	Verify that unused hardware devices have been disconnected from the network.		√	
18.3		**Physical access**			
18.3.2(b) Incremental 18.3.2(e) Incremental	18.3.2(a)-(c)	ISO/IEC 27001:2005 does not cover specific physical security controls within data centre. Determine if the following controls are in place: • Surveillance systems are monitoring access to and within the data centre and determine if sufficient data centre security has been implemented and is operational. • Access has been limited to authorised personnel on a need basis and upon termination or expiry of employment contract, the access is revoked. • The information processing facilities have appropriate controls in place to restrict or isolate all entry points with possibility of unauthorised entry. • Effective physical access controls are in place to restrict access to components, as stated in MTCS SS Audit Procedure 18.3.2(c), to authorised personnel only.		√	
18.4		**Visitors**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
18.4.2(a)-b) Incremental	18.4.2(a)-(b)	Determine if authorised visitors to the facility are escorted by authorised personnel and if there is an appropriate differentiation between visitors and on-site personnel.		√	
18.4.2(d) New	18.4.2 (e)	Determine if a detailed visitors' log is maintained and if the log includes the contents as stated in MTCS SS Audit Procedure 18.4.2(c). Verify that periodical reviews of visitors' logs have been performed.		√	
18.4.2(e) Incremental	18.4.2(d)	Determine if appropriate restrictions for all publicly accessible network points are in place.		√	
18.5		**Environmental threats and equipment power failures**			
18.5.2(b) New 18.5.2(c)-(d) Incremental 18.5.2(f)-(h) Incremental	18.5.2(b)-(g)	Verify that controls as stated in MTCS SS Clause s 18.5.2(b)-(d) and 18.5.2(f)-(h) have been implemented.		√	
18.6		**Physical security review**			
18.6.2(a) Incremental 18.6.2(b) Incremental	18.6.2(a)	Inspect the outcome of the physical security review and verify if the assessment covers those areas as stated in MTCS SS Requirement 18.6.2(a). Verify if security reviews have been conducted at least on a yearly basis.	√		
19		**Operations**			
19.2		**Documentation of service operations and external dependencies**			
19.2.2(a) Incremental	19.2.2(a)	ISO/IEC 27001:2005 does not cover cloud specific documentations. Determine if documentations on the operation of cloud services are complete and up-to-date.	√		
19.3		**Capacity management**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
19.3.2(a) Incremental	19.3.2(a)	Determine if the Cloud Service Provider has a capacity management plan and documented projections on the future capacity requirements to ensure that the availability, quality and adequacy of capacity and resources in accordance with regulatory and contractual requirements.	√		
20		**Change management**			
20.2		**Backup procedures**			
20.2.2(a) Incremental	20.2.2(a)	ISO/IEC 27001:2005 does not cover backup procedures for systems / applications. Verify that there are procedures in place for the Cloud Service Provider to perform backups of affected systems or applications prior to the change.	√		
20.5		**Patch management procedures**			
20.5.2(a)-(b) Incremental	20.5.2(a)	ISO/IEC 27001:2005 does not cover patch management procedures and hardening standards for dormant / offline systems. Determine if patch management procedures are in place. Conduct system configuration reviews to ensure the latest patches are applied to the systems or devices according to the procedures. Also, verify if there is a process or procedure in place to ensure that systems that have been dormant or offline for a period of time have been configured to meet hardening requirements as specified in MTCS SS Clause 20.5.2(b).	√	√	
21		**Business continuity planning (BCP) and disaster recovery (DR)**			
21.2		**BCP and DR plans**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
21.2.2(a)-(b) Incremental	21.2.2(a)-(b)	Determine if risk assessments conducted include the identification of events that can cause interruptions to business processes and assesses the need for BCP and DR plans based on the criticality of the system / application. Determine if roles and responsibilities for BCP and DR have been established in sufficient detail.	√		
21.3		**BCP and DR testing**			
21.3.2(a) Incremental	21.3.2(a)-(b)	Determine if an appropriate frequency has been defined for the testing and update of BCP and DR plans, and if BCPs are updated and tested according to the frequency.	√		
22		**Cloud services administration**			
22.1		**Privilege account creation**			
22.1.2(c) Incremental 22.1.2(d) New	22.1.2(c)-(d)	ISO/IEC 27001:2005 does not explicitly cover controls in MTCS SS Clause s 22.1.2(c)-(d) for privileged account management. Determine if a process or procedure is in place for the management to approve the granting of privileged accounts that have access to the cloud infrastructure and verify that these accounts are not being used as system or service accounts.	√	√	
22.2		**Generation of administrator passwords**			
22.2.2(a)-(c) Incremental	22.2.2(a)-(b)	ISO/IEC 27001:2005 does not cover specific details on administrator passwords. Verify that following requirements, as defined in MTCS SS Clause 22.2.2(a)-(c) are part of hardening documents and have been implemented: • minimum password criteria are aligned with industry standard practices, • generic passwords are disallowed; and • shared passwords with other accounts are disallowed.	√	√	
22.3		**Administrator access review and revocation**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.3.2(c) Incremental	22.3.2(c)	Verify that inactive accounts are removed or disabled at least every ninety (90) days and relevant parties have been notified.		√	
22.4		**Account lockout**			
22.4.2(a)-(b) New	22.4.2(a)-(b)	ISO/IEC 27001:2005 does not cover account lockout. Verify if configurations to lock an account after a maximum of six (6) unsuccessful attempts and lockout duration to be a minimum of thirty (30) minutes are part of hardening documents and have been implemented.		√	
22.5		**Password change**			
22.5.2(a) New 22.5.2(b) Incremental	22.5.2(a)-(b)	ISO/IEC 27001:2005 does not cover details on password change. Determine if configurations and hardening guidelines are in place to enforce compulsory password change based on industry standard practices and ensure that while changing the password, previous three passwords cannot be used.		√	
22.6		**Password reset and first logon**			
22.6.2(a)-(c) Incremental 22.6.2(d) New	22.6.2(a)	ISO/IEC 27001:2005 does not cover user access management details and two factor authentication. Determine if the following configurations are in place: • generation of unique passwords and mandating password change upon first login, • verification of identity prior to changing password, • obtaining of management approval in the event of a password reset via configurations in systems or policies and procedures; and • process or procedure for the reset of password in the event of the second factor device being lost.	√	√	
22.7		**Administrator access security**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.7.2(d) New 22.7.2(e) Incremental	22.7.2(d)	ISO/IEC 27001:2005 does not cover user access management details. Role based access control is not mentioned in ISO/IEC 27001:2005. Determine if explicit approval needs to be obtained for local administrative access and if role-based access control mechanisms are in place to control administrative access.	√	√	
22.8		**Administrator access logs**			
22.8.2(a) New	22.8.2(a)-(c)	ISO/IEC 27001:2005 does not cover establishment of procedures to review administrator activities. Determine if a process or procedure is in place to review all administrator activities periodically.	√		
22.9		**Session management**			
22.9.2(b) Incremental	22.9.2(a)-(c)	Determine if configurations are in place to require the re-entering of passwords for reactivation of terminals that have been inactive for more than fifteen (15) minutes.	√	√	
22.10		**Segregation of duties**			
22.10.2(a)-(c) Incremental	22.10.2(a)-(c)	ISO/IEC 27001:2005 does not cover specific operational procedures and responsibilities. Determine if the following controls are in place: • Risks reviews are conducted for access rights and segregation of duties. • Appropriate restrictions are in place to control movement of object codes between different environments. • Appropriate restrictions are in place to control access to backup and production systems.	√	√	
22.11		**Secure transmission of access credentials**			
22.11.2(a) New	22.11.2(a)-(c)	Verify that no clear-text protocols or weak encryption is used for administrative access by reviewing approved system hardening documents and testing.		√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.12		**Third party administrative access**			
22.12.2(a) Incremental	22.12.2(a)-(c)	Verify that privileged access for vendors is controlled on a 'need-to-have' basis via the approved hardening documents and actual system configurations.	√	√	
22.13		**Service and application accounts**			
22.13.2(a) Incremental	22.13.2(a)	Verify that all service and application accounts created meet the requirements as stated in MTCS SS Requirement 22.13.2(a).	√	√	
23		**Cloud user access**			
23.2		**User access security**			
23.2.2(a) Incremental 23.2.2(c) New	23.2.2(a)-(c)	In addition to user access management in ISO/IEC 27001:2005 Clause A.11.2, requirements pertaining to user access to the cloud environment as defined in MTCS SS Clause s 23.2.2(a), 23.2.2(c) and 23.2.2(e) shall be enforced by the Cloud Service Provider.		√	
23.2.2(e) New	23.2.2(e)	Verify that the following have been enforced: • documented approval from authorised personnel for granting of user access privileges, • default "deny-all" setting; and • implementation of anti-bot controls to foil automated brute force attacks.			
23.3		**User access password**			
23.3.2(a)-(c) Incremental	23.3.2(a)-(b)	Verify that, in addition to, the user responsibilities in ISO/IEC 27001:2005 Clause A.11.3, minimum password criteria shall follow industry standard practices as stated in MTCS SS Requirement 23.3.2(a). In addition, verify generic passwords and shared passwords are disallowed.		√	
23.4		**User account lockout**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.4.2(a) New 23.4.2(b) New	23.4.2(a)-(b)	Verify that requirements, as specified in MTCS SS Clauses 23.4.2(a)-(b) are in place to lock an account after a maximum of six unsuccessful attempts and lockout duration to be a minimum of thirty (30) minutes.		√	
23.5		**User password reset and 1st logon change**			
23.5.2(a)-(b) Incremental	23.5.2(a)-(b)	Determine if configurations are in place to ensure that: • unique passwords are generated, • password change upon first login is mandated; and • users have to verify their identities prior to the changing of passwords.	√	√	
23.6		**Password protection**			
23.6.2(a) Incremental 23.6.2(b) Incremental 23.6.2(c) New	23.6.2(a)-(b)	Verify the following password configuration, as specified in MTCS SS Audit Procedures 23.6.2(a)-(b) have been implemented: • passwords are rendered unreadable during transmission as defined in hardening documents, • passwords are transmitted through encrypted channels as defined in hardening documents; and • passwords are protected through the encryption of password storage as defined in hardening documents.		√	
23.7		**User session management**			
23.7.2(b) Incremental 23.7.2(c) Incremental	23.7.2(a)-(b)	Determine if the following configurations, as documented in hardening guidelines, have been implemented: • re-entering of passwords for reactivation of terminals that have been inactive for more than fifteen (15) minutes; and • cryptographically strong session identifiers.		√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.9		**Self-service portal creation and management of user accounts**			
23.9.2(a) Incremental	23.9.2(a)	Verify that strict password controls are in place as defined in MTCS SS Requirement 23.3.		√	
23.10		**Communication with cloud users**			
23.10.2(a) New	23.10.2(a)	Determine if a method for securely distributing official notifications has been defined and implemented.		√	
24		**Tenancy and customer isolation**			
24.1		**Multi tenancy**			
24.1.2(c) Incremental	24.1.2(c)	ISO/IEC 27001:2005 does not cover multi tenancy and segregation between virtual machines belonging to different users. Determine if segregation between virtual machines belonging to different users has been enforced.	√	√	
24.3		**Network protection**			
24.3.2(d) Incremental 24.3.2(e) New	24.3.2(a)-(g)	ISO/IEC 27001:2005 does not cover network protection characteristics for the cloud infrastructure. Determine if the following controls are in place: • comparisons have been made for critical network infrastructure configurations against standards for each type of network device and deviations from the baselines are documented, approved and undone when not required, • network environment has been reviewed at regular planned intervals, • high-risk environments and data flow network	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
24.3.2(f) Incremental 24.3.2(j)-(l) New		architecture diagrams that may have regulatory compliance impact have been clearly identified, • multi-factor authentication for remote user access has been implemented, • access to the virtualisation layer has been restricted, • multi-factor and / or split control authentication have been implemented to restrict access to hypervisor; and • remote management of hypervisor for cloud implementation using virtualisation technology has been disabled.			
24.4		**Virtualisation**			
24.4.2(a)-(c) Incremental	24.4.2(a)-(b)	ISO/IEC 27001:2005 does not cover specific virtualisation related features. Verify if the following controls have been implemented: • Cloud Service Provider has maintained a list of virtualised IT systems and services. • Security risks and vulnerabilities that can be exploited from the use of virtualisation have been identified and addressed appropriately. • Risk assessment and treatment has been performed for these virtualised IT systems and services covering at least the areas as stated in MTCS SS Requirement 24.4.2(a). • Systems and services have been appropriately encrypted to protect against virtual machine theft.	√	√	
24.5		**Storage area networks (SAN)**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
24.5.2(b) Incremental	24.5.2(b)	ISO/IEC 27001:2005 does not cover equipment security for SAN. Determine if a process or procedure is in place to propagate all configuration changes and verify that configurations for the SAN and associated switches have been performed correctly.	√	√	

8.2 MTCS SS Level 2

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

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6		**Information security management**			
6.4		**Information Security Policy**			
6.4.2(b) Incremental	6.4.3(a)-(c)	ISO/IEC 27001:2005 does not cover all the details pertaining to development of a strategic plan. Determine if the strategic plan and security policy are reviewed and updated regularly, and are well understood by relevant personnel and third-parties. Also, determine if the strategic plan and security policy covers key cloud computing risks relevant to the organisation.	√		
6.6		**Information security audits**			
6.6.2(a) Incremental	6.6.3(a)	ISO/IEC 27001:2005 does not cover the establishment of an audit committee. Assess the audit staff's understanding of the risks relevant to the organisation.	√		√
6.7		**Information security liaisons (ISL)**			
6.7.3(a) New	6.7.3(a)	In addition to ISO/IEC 27001:2005 Clauses A.6.1.6 and A.6.1.7, determine if the designated information security liaison is available for contact by customers by verifying that the Cloud Service Provider has provided an information security contact for customers through appropriate channels.	√		
6.8		**Acceptable Usage**			
6.8.3(a) Incremental	6.8.3(a)	ISO/IEC 27001:2005 does not include the details for the acceptable network locations. Determine if labelling for devices have been done appropriately based on the Cloud Service Provider's data classification policy and if a list of acceptable network locations for the components as stated	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6.8.3(b) Incremental		in MTCS SS Requirement 6.8.3(a) is available. In addition, determine if a process or procedure is in place to obtain explicit authorisation for personnel accessing customer data for purposes as stated in MTCS SS Requirement 6.8.3(b).			
7		**Human resources**			
7.1		**Background screening**			
7.1.3(a) Incremental	7.1.3(a)	ISO/IEC 27001:2005 does not cover frequency of background screening. Verify that at least one (1) annual background has been conducted for personnel with access to the networks as stated in MTCS SS Requirement 7.1.3(a).	√		
7.2		**Continuous personnel evaluation**			
7.2.3(a) Incremental	7.2.3(a)	ISO/IEC 27001:2005 does not cover frequency of continuous personnel evaluation. Verify that annual evaluations have been conducted for personnel with access to the networks as stated in MTCS SS Requirement 7.2.3(a).	√		
7.2.3(b) Incremental	7.2.3(b)	ISO/IEC 27001:2005 does not cover the scope of coverage of the personnel evaluation. Determine if the evaluation for personnel include at least the requirements as stated in MTCS SS Requirement 7.2.3(b).	√		
7.6		**Information security training and awareness**			
7.6.3(a) Incremental	7.6.3(a)-(b)	ISO/IEC 27001:2005 does not cover the specific topic on the sensitive data in cloud environment and the communication of data protection policies to relevant parties. Determine if awareness has been created on the importance of	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
7.6.3(c) Incremental		information security for sensitive data in the cloud environment and if data protection policies have been communicated to employees and relevant third parties. In addition, determine if there are controls to ensure that the security training scope, material and schedule are approved by the management.			
7.6.3(d) Incremental 7.6.3(e) Incremental	7.6.3(c)	ISO/IEC 27001:2005 does not cover the specific topic on personal data and Computer Misuse Act as part of the awareness program. Determine if the relevant elements of the Computer Misuse Act have been taken into consideration when developing the materials for information security training and awareness.	√		
8		**Risk management**			
8.1		**Risk management program**			
8.1.3(a) Incremental	8.1.3(a)-(b)	ISO/IEC 27001:2005 does not specify the categories of risk criteria in the risk management program. Verify that acceptance levels based on risk criteria listed in MTCS SS Requirement 8.1.3(a) have been established and documented with reasonable resolution time frames and approved by management.	√		
8.2		**Risk assessment**			
8.2.3(a) Incremental	8.2.3(a)	ISO/IEC 27001:2005 does not specifically include data protection requirements in the risk assessments. Determine if data protection requirements have been taken into consideration during risk assessments.	√		
8.3		**Risk management**			
8.3.3(a) Incremental	8.3.3(b)	ISO/IEC 27001:2005 does not specify the prioritization of material risks. Verify that all material risks have been evaluated and prioritised, and the results be endorsed by relevant parties.	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
8.3.3(d) Incremental	8.3.3(c)	ISO/IEC 27001:2005 does not cover the development of a strategy for the risk remediation. Determine if a strategy has been developed to address and mitigate the risks. In addition, assess if any systems implemented based on the strategy developed are able to mitigate risks identified.	√		
8.4		**Risk register**			
8.4.3(a) Incremental	8.4.3(a)	ISO/IEC 27001:2005 does not specify the establishment of a risk register containing the risk attributes stated in the MTSC SS Requirement 8.4.3(a). Determine if the risk attributes as stated in MTCS SS Requirement 8.4.3(a) have been appropriately defined by the Cloud Service Provider in their risk register.	√		
9		**Third party**			
9.1		**Third party due diligence**			
9.1.2(a) Incremental	9.1.3(a)	ISO/IEC 27001:2005 does not cover specific criteria for third party due diligence. Determine if sufficient due diligence (with components as stated in MTCS SS Requirement 9.1.2(a)) has been carried out before appointing a third party service provider. Sample the output from the due diligence process to ensure that it adequately captures the requirements of the as stated in MTCS SS Requirement 9.1.2(a).	√		√
9.3		**Third party agreement**			
9.3.3(a) Incremental	9.3.3(a)	ISO/IEC 27001:2005 does not cover all detailed attributes as stated in MTCS SS Requirement 9.3.3(a). Determine if the attributes as stated in MTCS SS Requirement 9.3.3(a) have been appropriately addressed in the service level agreement with the third party service provider.	√		
9.4		**Third party delivery management**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
9.4.3(a) Incremental	9.4.3(a)	ISO/IEC 27001:2005 does not specify the third parties implementation details with the examples as stated in the MTCS SS Requirement 9.4.3(a). Determine if processes or procedures are in place to manage third parties and sub-contractors.	√		
9.4.3(b) Incremental	9.4.3(b)	ISO/IEC 27001:2005 does not specify the implementation and compliance of the data protection controls for Cloud Service Providers. Determine if data protection controls have been implemented and are compliant in accordance with regulatory requirements.	√		
10		**Legal and compliance**			
10.1		**Compliance with regulatory and contractual requirements**			
10.1.3(a) Incremental	10.1.3(a)-(b)	ISO/IEC 27001:2005 does not specify the approach and coverage for the review and update. Determine if an approach has been developed by the Cloud Service Provider to periodically review and update documentation for each category of information system elements.	√		
10.2		**Compliance with policies and standards**			
10.2.3(a) Incremental	10.2.3(a)	ISO/IEC 27001:2005 does not specify the review and audit of compliance activities for Cloud Service Providers. Determine if independent parties have verified that the Cloud Service Provider is compliant with organisational policies by reviewing the internal audit plans.	√		
10.3		**Prevention of misuse of cloud facilities**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
10.3.2(a)-(b) Incremental	10.3.3(a)	ISO/IEC 27001:2005 does not cover the enforcement of acceptable use policy regarding cloud specific requirements on the awareness of the cloud environment's permitted access and use, and the monitoring policies, procedures and tools in place. Determine, through interviews, if employees understand requirements as stated in MTCS SS Clauses 10.3.2(a)-(b).	√		
10.6		**Continuous compliance monitoring**			
10.6.3(a) New	10.6.3(a)	ISO/IEC 27001:2005 does not cover the reporting requirements for system access. Verify that a mechanism has been implemented by the Cloud Service Provider to provide system access reports within an agreed upon timeframe to cloud users by determining the availability of system access reports.	√		
11		**Incident management**			
11.1		**Information security incident response plan and procedures**			
11.1.3(a) Incremental	11.1.3(a)	ISO/IEC 27001:2005 does not cover the development of incident response plan and procedures. Determine if personnel have been designated to be available to respond to security alerts from intrusion detection, intrusion prevention and file integrity monitoring systems in a timely manner.	√		
11.1.3(d) Incremental	11.1.3(d)	ISO/IEC 27001:2005 does not cover the development of an incident response plan and procedures. Determine if a process or procedure is in place for the:	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
11.1.3(e) Incremental		• escalation of events as to contain and remediate the breach; and • notification to customers and affected parties of incidents and the impact of the incidents, including the planned course of action for remediation.			
11.2		**Information security incident response plan testing and updates**			
11.2.3(a) Incremental	11.2.3(a)-(c)	ISO/IEC 27001:2005 does not cover the testing and updates of incident response plan. Determine if a process or procedure is in place to maintain information security incident response plan up-to-date in accordance with industry standards.	√		
11.3		**Information security incident reporting**			
11.3.2(b) Incremental	11.3.3(a)	ISO/IEC 27001:2005 does not cover the notification and provision of support to the relevant cloud users and third parties affected during a security breach. Perform tests to validate if the incident response reporting process is effective as per requirements in MTCS SS Clause s 11.3.2(a)-(b).	√		√
11.4		**Problem management**			
11.4.3(a) Incremental	11.4.3(a)-(c)	ISO/IEC 27001:2005 does not specify the requirement for a trend analysis of the incidents. Verify that a quarterly trend analysis of past incidents has been developed by inspecting the trend analysis documents and determining if all material incidents are considered in the analysis.	√		
12		**Data Governance**			
12.1		**Data classification**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.1.3(c) Incremental	12.1.3(a)-(b)	ISO/IEC 27001:2005 does not specify the classification of communication channels. Determine if communication channels have been appropriately classified such that the sensitivity of the communication channel could be determined for secure and insecure data transmission.	√		
12.3		**Data integrity**			
12.3.3(b) Incremental	12.3.3(b)	ISO/IEC 27001:2005 does not specify authenticity. Verify that appropriate controls have been implemented to protect authenticity and message integrity.	√	√	
12.4		**Data labeling / handling**			
12.4.3(a) Incremental	12.4.3(a)	ISO/IEC 27001:2005 does not specify the requirement on the maintenance logs of all media. Verify that inventory logs of all media (e.g., tape drives, backup drives) have been maintained.	√		
12.4.3(c) New	12.4.3(b)	Determine if the location where data is stored has been specified by the Cloud Service Provider in accordance in the agreement with customers and verify that these locations have been pre-agreed by the user.		√	
12.5		**Data protection**			
12.5.3(a) Incremental	12.5.3(b)	ISO/IEC 27001:2005 does not require a review of the physical storage security. Verify that the security of the physical storage of media is reviewed annually. Determine if the distribution of any kind of media is strictly prohibited unless compelled by laws or regulations.	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.5.3(b) Incremental	12.5.3(c)	ISO/IEC 27001:2005 does not cover all the security mechanisms as stated in MTCS SS Requirement 12.5.3(b). Verify that appropriate security mechanisms have been implemented to monitor access to data in order to prevent data leakage. The security mechanisms should include, but not be limited to, those as stated in MTCS SS Requirement 12.5.3(b).		√	
12.5.3(c) Incremental	12.5.3(d)	ISO/IEC 27001:2005 does not specify the encryption requirements for end point devices. Verify that strong encryption has been implemented for all end point devices handling customer data.		√	
12.5.3(d) Incremental	12.5.3(a)	ISO/IEC 27001:2005 does not cover the security controls for virtualised images and snapshots. Verify that appropriate security controls have been implemented for those as stated in MTCS SS Requirement 12.5.3(d).		√	
12.6		**Data retention**			
12.6.3(a) Incremental	12.6.3(a)-(b)	ISO/IEC 27001:2005 does not include the requirements on backup or redundancy mechanisms. Verify that backup or redundancy mechanisms have been implemented in accordance with legal, regulatory, and business requirements.	√		
12.6.3(d) Incremental	12.6.3(c)	ISO/IEC 27001:2005 does not specify the mechanisms and rules for retention. Determine if processes or procedures are in place to periodically identify and delete all data that exceeds defined retention requirements.	√	√	
12.8		**Secure disposal and decommissioning of hardcopy, media and equipment**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.8.2(c) New	12.8.3(a)	Secure disposal and decommissioning procedures of hardcopy materials are not mentioned in ISO/IEC 27001:2005. Verify, through interviews, if relevant personnel understands the disposal processes and roles in the processes.	√		
12.9		**Secure disposal verification of live instances and backups**			
12.9.3(a) Incremental	12.9.3(a)-(c)	ISO/IEC 27001:2005 does not include the requirement to verify that data has been securely removed. Determine if a process or procedure is in place to verify the removal of data from the entire cloud environment, including live instance / snapshots, dormant virtual machines and backups, when it is deleted. Also, verify that verification of such secure disposals has been performed and documented.	√	√	
12.10		**Tracking of data**			
12.10.3(a) New	12.10.3(a)-(b)	ISO/IEC 27001:2005 does not specify cloud users are able to track the locations of data. Verify that location information of all data in production and backup environment are available to cloud users by identifying the facilities provided to track data and determining the accuracy of the reporting.	√	√	
12.11		**Production data**			
12.11.3(a) Incremental	12.11.3(a)	ISO/IEC 27001:2005 does not cover tracking of data for operational procedures. Verify that appropriate controls have been implemented to prohibit the extraction or transfer of production data to non-production media, systems, or environments that do not have the same controls as production.	√	√	
12.11.3(b) Incremental	12.11.3(b)	ISO/IEC 27001:2005 does not cover internal processes for duplicating production data. Determine if an internal approval process or procedure is in place for the duplication of production data.	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.11.3(c) Incremental 12.11.3(d) Incremental	12.11.3(c)-(d)	ISO/IEC 27001:2005 does not cover tracking of data for operational procedures and electronic commerce services. Determine if a process or procedure is in place to perform sanitisation and obtain approval before allowing usage of production data in non-production environments, and if the policy regarding copying data into non-production environments by the Cloud Service Provider has been communicated.	√	√	
13		**Audit logging and monitoring**			
13.1		**Logging and monitoring process**			
13.1.3(d) Incremental 13.1.3(e) New	13.1.3(d)	ISO/IEC 27001:2005 does not cover the implementation of software to detect unauthorised changes to logs and the implementation of Intrusion Detection and Prevention Systems (IDPS). Verify that file integrity monitoring or change detection software on logs and IDPS have been implemented and configured as specified in hardening documents.		√	
13.2		**Log review**			
13.2.3(a) Incremental	13.2.3(a)-(d)	ISO/IEC 27001:2005 does not cover the frequency of log review. Verify that log reviews have been performed for all system components at least on a daily basis.	√	√	
13.3		**Audit trails**			
13.3.3(a) Incremental	13.3.3(a)	ISO/IEC 27001:2005 does not specify the media to be used for capturing audit trails. Verify that audits trails are only written to write-only media or a tamper resistant location that prevents modifications.		√	
13.4		**Backup and retention of audit trails**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
13.4.3(a) Incremental	13.4.3(a)-(e)	ISO/IEC 27001:2005 does not cover the backup requirements for logs. Verify that audit trails are backed up regularly to a centralised log server or media accessible only by authorised personnel by determining if the log server is located on an internal network segment.		√	
14		**Secure configuration**			
14.2		**Malicious code prevention**			
14.2.2(b)-(g) Incremental	14.2.3(a)	ISO/IEC 27001:2005 does not cover specific control requirements for malicious code prevention. Refer to MTCS SS Audit Procedures 14.2.2(a)-(g) for specific audit procedures regarding malicious code prevention. Determine if relevant personnel understand malicious code prevention techniques and practices as defined by the organisation.	√	√	
14.7		**Unnecessary service and protocols**			
14.7.3(a) Incremental	14.7.3(a)	ISO/IEC 27001:2005 does not include the requirements on unnecessary service and protocols. Conduct system configuration reviews to determine that all unnecessary functionalities, such as scripts, drivers, features, subsystems, file systems and unnecessary web servers have been removed.		√	
14.9		**Enforcement checks**			
14.9.3(a) Incremental	14.9.3(a)-(b)	ISO/IEC 27001:2005 does not specify the frequency of compliance checks. Verify that enforcement checks are done at least once in a week to ensure that all security configurations are applied according to baseline standards. Review the enforcement check reports.	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14.9.3(b) New	14.9.3(c)	ISO/IEC 27001:2005 does not require the implementation of file integrity monitoring tools. Determine if sufficient file integrity monitoring tools to compare and alert unauthorised modification of critical system and content file have been implemented.		√	
15		**Security testing and monitoring**			
15.1		**Vulnerability scanning**			
15.1.3(a) Incremental	15.1.3(a)	ISO/IEC 27001:2005 does not specify the mechanisms and frequency for vulnerability assessment. Determine if internal and external vulnerability scans have been conducted at least on a quarterly basis (e.g., review vulnerability assessment reports, scan results).	√		√
15.1.3(b) Incremental	15.1.3(b)	ISO/IEC 27001:2005 does not specify the usage of the Common Vulnerability Scoring System (CVSS) to address vulnerabilities timely. Review a sample of scan results and ensure that vulnerabilities with a CVSS score of 4 – 6.9 were addressed within a month of detection of the vulnerability.		√	
16		**System acquisitions and development**			
16.1		**Development, acquisition and release management**			
16.1.3(a) New	16.1.3(a)-(b)	ISO/IEC 27001:2005 does not cover the verification of the integrity and authenticity of the applications. Verify that protection controls which allow the clients to verify the integrity and authenticity of the applications have been implemented. Examine if proper test cases have been developed and sign-off has been performed for changes / new development of a system. Determine if developers understand secure coding practices.	√	√	√
16.2		**Web application security**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
16.2.3(a) Incremental 16.2.3(c) New	16.2.3(a)	ISO/IEC 27001:2005 does not cover the review of web applications using assessment tools and testing of public web services. Determine if the following controls are in place: • Application security assessment performed annually or when there are changes to the applications using manual or automated application vulnerability security assessment tools or mechanisms, covering at least common web application flaws. • Security assessments include at the minimum, the identification of common web application flaws. • Inclusion of public web services in security testing.	√		
16.3		**System testing**			
16.3.3(a) Incremental	16.3.3(a)-(c)	ISO/IEC 27001:2005 does not include the systematic monitoring and evaluation program for all the areas as stated in MTCS SS Requirement 16.3.3(a). Verify that a systematic monitoring and evaluation program to ensure that software development is performed in accordance with industry standards and regulatory requirements has been implemented by the Cloud Service Provider. The program should include, but not be limited to, the requirements as stated in MTCS SS Requirement 16.3.3(a).	√	√	
16.4		**Source code security**			
16.4.2(a) Incremental	16.4.3(a)-(b)	ISO/IEC 27001:2005 does not cover version control. Determine, through interviews, if relevant personnel understand software version control and source code security requirements as stated in MTCS SS Requirement 16.4.2(a).	√		
16.5		**Outsourced software development**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
16.5.3(a) Incremental	16.5.3(a)-(b)	ISO/IEC 27001:2005 does not include the specific objective to ensure performance. Determine if a systematic monitoring and evaluation program to ensure that outsourced software development is performed in accordance with industry standards and regulatory requirements has been established by the Cloud Service Provider. Inquire if monitoring program is present to evaluate, monitor, and review outsourced software development. Review reports of the monitoring program to assess if all the recommended controls were followed.	√	√	
17		**Encryption**			
17.1		**Encryption policies and procedures**			
17.1.2(a)-(b) Incremental	17.1.3(a)	Determine, through interviews, if system administrators understand encryption requirements which include, at a minimum, those as stated in MTCS SS Clauses 17.1.2(a)-(b).	√		
17.2		**Channel Encryption**			
17.2.2(a) Incremental	17.2.3(a)	ISO/IEC 27001:2005 does not cover specific usage of encryption. Determine, through interviews, if system administrators understands methods used for accessing systems and whether those access methods are appropriately encrypted.	√		
17.3		**Key management**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
17.3.3(a) Incremental	17.3.3(a)-(c)	ISO/IEC 27001:2005 does not cover specific key management lifecycle process and controls. Determine if access controls are in place to access the cryptographic keys to minimise the number of custodians and prevent unauthorised substitution of keys. Review the access-list to the cryptographic keys and determine if each person in the list has been approved and has a valid business case to gain access to the keys.	√	√	
17.3.3(b) Incremental 17.3.3(c) Incremental	17.3.3(d)	ISO/IEC 27001:2005 does not cover specific key management lifecycle process and controls. Determine if cryptographic keys are stored in limited secured locations and if periodical security review of the cryptosystem has been conducted to evaluate key strength.	√	√	
17.3.3(d) Incremental 17.3.3(e) Incremental	17.3.3(e)	ISO/IEC 27001:2005 does not cover specific key management lifecycle process and controls. Verify that old cryptographic keys are archived securely and only used for decrypting purposes. Determine if clear-text key management is implemented. In addition, verify if any one person can have full knowledge of cryptographic keys and if dual control on crypto-keys is enforced.	√	√	
17.3.3(f) Incremental 17.3.3(g)-(h) Incremental	17.3.3(f)	ISO/IEC 27001:2005 does not cover specific key management lifecycle process and controls. Determine if policies and standards are established and implemented to manage logical access independently of native operating system access control mechanisms and verify that decryption keys are not tied to user accounts. Also, determine if private keys are generated individually on each device and verify that they cannot be exported from the device.	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
18		**Physical and environmental**			
18.1		**Asset management**			
18.1.3(a) New	18.1.3(a)	ISO/IEC 27001:2005 does not cover, as part of decommissioning, the control related to timely replacement of assets. Determine if there is a defined frequency to assess the assets and an established timeline to replace out-of-support information assets (e.g., within one (1) year from the date of end-of support) to support the decommissioning of out-of-support systems which might be exposed to security risks.	√		
18.3		**Physical access**			
18.3.3(a) Incremental	18.3.3(a)-(c)	ISO/IEC 27001:2005 does not include monitoring and storage of access logs. Determine if all individual access to areas hosting sensitive data is logged and access logs are stored for at least three (3) months. Determine if regular reviews of access logs are being conducted.	√	√	
18.4		**Visitors**			
18.4.3(a) Incremental	18.4.3(a)-(b)	ISO/IEC 2001:2005 does not include management approval as part of access control policy. Determine if management approval has been established as a prerequisite before visitors are allowed into facilities hosting sensitive data.	√	√	
19		**Operations**			
19.4		**Service levels**			
19.4.3(b) Incremental	19.4.3(b)	ISO/IEC 2001:2005 does not cover communication of contractual remedies. Determine if contractual remedies available to users have been communicated to them by examining a sample of communication between the Cloud Service Provider and cloud user.	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
19.4.3(c) Incremental	19.4.3(a)	ISO/IEC 2001:2005 does not include automation of alerts to the cloud user in the event of security breach or performance degradation. Determine if automated alerts for potential security issues, performance degradation, and other factors that may affect the cloud user have been communicated to the cloud user by reviewing the process for sending automated alerts to ensure it effectively captures key concerns.	√	√	
19.6		**Recoverability**			
19.6.3(a) Incremental 19.6.3(b) Incremental	19.6.3(a)-(b)	ISO/IEC 2001:2005 does not cover details related to alternate sites and point-in-time backup copies. Determine if a process has been established by the Cloud Service Provider to ensure high availability architecture of the infrastructure at the primary site and alternate site and if the availability of adequate point-in-time backup copies / snapshots of data for restoration to known consistent states are ensured.	√	√	
20		**Change management**			
20.1		**Change management process**			
20.1.3(a) Incremental	20.1.3(a)-(b)	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. Determine if procedures have been established by the Cloud Service Provider to inform affected cloud users and other third parties of changes.	√		
20.3		**Back-out or rollback procedures**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
20.3.3(a) Incremental	20.3.3(a)	ISO/IEC 2001:2005 does not cover rollback plans and procedures as part of backup management. Determine if a rollback procedure is established for the Cloud Service Provider to roll back to a former version if problem is encountered during or after the deployment of change. Sample changes which adversely affect the system and verify if rollbacks have been applied for those corresponding changes.	√	√	
20.5		**Patch management procedures**			
20.5.3(a) Incremental	20.5.3(a)	ISO/IEC 2001:2005 does not include the provision of risk ratings to vulnerabilities. Verify that newly discovered security vulnerabilities have been assigned risk ratings by reviewing files or reports that document newly discovered security vulnerabilities and the respective risk ratings.	√		
20.5.3(b) New	20.5.3(b)-(c)	ISO/IEC 2001:2005 does not cover the prioritisation and assignment of timeframes for patches. Determine if a risk-based approach has been approved and adhered to in prioritizing and defining a specific period to the application of security patches based on the level of criticality of the released patch addresses.	√		
20.5.3(c) New	20.5.3(d)	ISO/IEC 2001:2005 does not specify the testing of patches. Determine if testing is done by the Cloud Service Provider by reviewing the report that documents the result of the patch testing.	√		
20.5.3(d) Incremental	20.5.3(b)-(c)	ISO/IEC 2001:2005 does not cover hardening of dormant or offline systems. Verify that a process has been implemented by the Cloud Service Provider to ensure that systems that have been dormant or offline for over thirty days are configured to meet hardening standards and all security software including patches is up-to-date.	√	√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22		**Cloud services administration**			
22.2		**Generation of administrator passwords**			
22.2.3(a) Incremental	22.2.3(a)	ISO/IEC 27001:2005 does not cover specific details on administrator passwords. Verify that minimum password standards implemented meet or exceed the criteria which are aligned with industry standard practices.	√	√	
22.2.3(b)-(c) Incremental	22.2.3(b)-(c)	ISO/IEC 27001:2005 does not cover details on administrator passwords and two-factor authentication (2FA). Determine if 2FA is implemented for administrator accounts and if exceptions are approved and documented. Also, determine if the 2FA solution has been implemented by the Cloud Service Provider based on the 2FA vendor's recommended practices.	√	√	
22.4		**Account lockout**			
22.4.3(a) New	22.4.3(a)-(c)	ISO/IEC 2001:2005 does not cover details about account lockout. Verify that accounts that have been locked can only be unlocked by another administrator manually by reviewing the approved hardening documents and the system configuration.		√	
22.5		**Password change**			
22.5.3(a) New	22.5.3(a)	ISO/IEC 2001:2005 does not cover two-factor authentication (2FA). Determine if approved change management process and vendor recommended practices have been followed for 2FA key or token changes.	√	√	
22.6		**Password reset and first logon**			
22.6.3(a) Incremental	22.6.3(a)	ISO/IEC 2001:2005 does not cover the splitting of password. Verify that password reset processes require that the new password provided is split controlled and via out-of-band mechanism or other similar mechanisms.	√		
22.7		**Administrator access security**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.7.3(a) Incremental	22.7.3(a)-(b)	ISO/IEC 2001:2005 does not cover bastion hosts. Verify that access from the Cloud Service Provider Internal Network to the Cloud Service Management Network and Cloud Service Delivery Network is only permitted via bastion hosts by reviewing the infrastructure and logs to ensure that only defined IP addresses are allowed.	√	√	
22.8		**Administrator access logs**			
22.8.3(a) Incremental	22.8.3(a)	ISO/IEC 27001:2005 does not cover controls to prevent tampering and automatic alert or escalation of incidents concerning access control policies. Verify that controls have been implemented by the Cloud Service Provider to protect the logs from tampering by the administrators and to alert or escalate automatically any suspicious activities or violations to access control policies, especially by administrative accounts or machines, by reviewing system configuration, the escalation alerts and follow-up actions performed.	√	√	
22.9		**Session management**			
22.9.2(b) Incremental	22.9.3(a)	Determine, through interviews, if administrators understand relevant security controls for session management as stated in MTCS SS Clauses 22.9.2(a)-(b).	√		
22.10		**Segregation of duties**			
22.10.3(a) Incremental	22.10.3(a)	ISO/IEC 27001:2005 does not define frequency of review of access rights. Verify that risk reviews for access rights and segregation of duties are conducted at least on a quarterly basis.	√		
22.13		**Service and application accounts**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.13.3(a)-(e) Incremental	22.13.3(a)-(b)	ISO/IEC 27001:2005 does not cover detailed requirements pertaining to service and application accounts. Verify that the controls as stated in MTCS SS Clause s 22.13.3(a)-(e) to manage service and application accounts have been implemented by the Cloud Service Provider.	√	√	
23		**Cloud user access**			
23.2		**User access security**			
23.2.3(a) New	23.2.3(a)	ISO/IEC 27001:2005 does not cover two-factor authentication (2FA). Verify that a 2FA mechanism has been implemented or is available for cloud users.	√	√	
23.3		**User access password**			
23.3.3(a) Incremental	23.3.3(a)	ISO/IEC 27001:2005 does not define specific criteria for passwords. Verify that the minimum password criteria stated in MTCS SS Requirement 23.3.3(a) have been implemented by the Cloud Service Provider.		√	
23.4		**User account lockout**			
23.4.3(a)-(b) New	23.4.3(a)-(c)	ISO/IEC 27001:2005 does not cover details pertaining to account lockout. Verify that configurations are in place to lock an account after a maximum of six (6) unsuccessful attempts by reviewing the approved hardening documents and the system configuration. Also, verify that accounts are locked until an administrator enables the account by reviewing the approved hardening documents and the system configuration.		√	
23.6		**Password protection**			
23.6.2(a)-(b) Incremental 23.6.2(c) New	23.6.3(a)-(b)	Determine, through interviews, if administrators and developers understand password protection requirements as stated in MTCS SS Clauses 23.6.2(a)-(c).	√		
23.8		**Change of cloud user's administrator details notification**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.8.3(a)-(b) New	23.8.3(a)-(b)	Verify that a change in the cloud user's administrator details triggers an alert to the Cloud Service Provider's administrator and that the change in cloud user's administrator details can only be effected upon approval from the Cloud Service Provider's administrator.		√	
23.10		**Communication with cloud users**			
23.10.3(a) Incremental	23.10.3(a)	ISO/IEC 27001:2005 does not include specific topics for user education. Verify that education and training on relevant cloud security topics has been made available to cloud users.	√		
24		**Tenancy and customer isolation**			
24.2		**Supporting infrastructure segmentation**			
24.2.3(a) Incremental	24.2.3(a)	ISO/IEC 27001:2005 does not include the separation of authentication sources. Verify that the authentication sources for Cloud Service Delivery Networks and the Cloud Service Provider Internal Networks are separated.	√	√	
24.2.3(c) Incremental	24.2.3(b)-(c)	ISO/IEC 27001:2005 does not include two-factor authentication (2FA). Verify that the Cloud Management Networks and Cloud Service Provider Internal Networks are segmented and only controlled access point with 2FA is allowed.	√	√	
24.3		**Network protection**			
24.3.3(c) Incremental 24.3.3(d)-(e) New	24.3.3(a)	ISO/IEC 27001:2005 does not cover network protection characteristics for the cloud infrastructure. Verify if the following controls have been implemented: • direct public access to systems hosting sensitive data is prohibited, • stateful inspection is implemented; and • disclosure of internal IP address is prevented.		√	
24.5		**Storage area networks (SAN)**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
24.5.3(c) New 24.5.3(e) New	24.5.3(a)	ISO/IEC 27001:2005 does not cover equipment security for SAN. Determine, by reviewing the SAN configurations, if: • mutual authentication between devices on a SAN is being leveraged; and • automatic replication for data stored on a SAN is disallowed.	√	√	
24.6		**Data segregation**			
24.6.3(a) Incremental 24.6.3(b) Incremental	24.6.3(a)	ISO/IEC 27001:2005 does not cover segregation of data access among customers. Determine if minimum logical segregation for data access, logs, and encryption keys has been performed by the Cloud Service Provider, and verify that the Cloud Service Provider's offsite data storage and recovery have at least the same, or similar, level of segregation.	√	√	

8.3 MTCS SS Level 3

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

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6		**Information security management**			
6.4		**Information security policy**			
6.4.2(b) Incremental	6.4.4(a)-(b)	ISO/IEC 27001:2005 does not cover all the development of a strategic plan. Validate if there is an effective process to monitor the compliance of the Information Security Policy which is supported by an appropriate strategic plan and security program.	√		
7		**Human resources**			
7.1		**Background screening**			
7.1.4(a) Incremental	7.1.4(a)-(b)	ISO/IEC 27001:2005 does not cover frequency of background screening. Verify that at least one (1) annual background check is carried out for all relevant personnel and verify if the checks have been approved by the management.	√		
7.2		**Continuous personnel evaluation**			
7.2.4(a) Incremental	7.2.4(a)	ISO/IEC 27001:2005 does not cover frequency of continuous personnel evaluation. Verify that the annual evaluation is performed for all personnel security.	√		
7.3		**Employment and contract terms and conditions**			
7.3.4(a) Incremental	7.3.4(a)	ISO/IEC 27001:2005 does not include re-acknowledgement. Verify that the re-acknowledgement of acceptance of Information Security Obligations Agreement, as specified in MTCS SS Audit Procedure 7.3.4(a), is performed annually (in addition to the pre-employment contract), and prior to termination of service.	√		
7.6		**Information security training and awareness**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
7.6.3(a) Incremental 7.6.3(c)-(e) Incremental	7.6.4(a)-(c)	ISO/IEC 27001:2005 does not cover the specific topics mentioned in MTCS SS Clauses 7.6.3(a) and 7.6.3(c)-(e) as part of the awareness program. Determine that following controls have been implemented for the information security training sessions: • management has provided inputs in the curriculum creation, • curriculum highlights relevant training areas as stated in MTCS SS Clause 7.6.3.; and • employees and relevant third parties understand the topics covered in the session.	√		
8		**Risk management**			
8.1		**Risk management program**			
8.1.4(a) Incremental	8.1.4(a)-(b)	ISO/IEC 27001:2005 does not cover the specific frequency evaluation. Verify that the Cloud Service Provider has conducted evaluation of its risks at least on a quarterly basis and the scope of such evaluation includes the following, but not limited to: • risk metrics, • mitigation steps; and • plans to address residual risk. Based on the results, assess the security strategy to validate if the outcome of the risk assessment has been incorporated.	√		√
8.2		**Risk Assessment**			
8.2.3(a) Incremental	8.2.4(a)	ISO/IEC 27001:2005 does not cover cloud specific areas in the general ISMS risk assessment. Review the risk assessment process and ensure the controls,as specified in MTCS SS Audit Procedure 8.2.4(a) have been implemented.	√		

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
8.3		**Risk management**			
8.3.4(a) Incremental	8.3.4(a)-(b)	ISO/IEC 27001:2005 does not cover the IT risk metrics. Determine if the Cloud Service Provider has developed and approved IT risk metrics that are aligned with industry practices.	√		√
8.4		**Risk register**			
8.4.3(a) Incremental	8.4.4(a)	ISO/IEC 27001:2005 does not specify the establishment of a risk register containing the risk attributes stated in the MTSC SS Requirement 8.4.3(a) in the risk management. Review if the audit procedure, as defined in MTCS SS Clause 8.4.4(a) has been implemented.	√		
9		**Third party**			
9.2		**Identification of risks related to third parties**			
9.2.4(a)-(b) New	9.2.4(a)-(c)	If a third party service provider provides data centre facilities, determine if Threat and Vulnerability Risk Assessments (TVRAs) have been conducted by the third party service provider. Determine if the third party service provider has a remediation plan following a TVRA and has made available such a plan to the Cloud Service Provider. In addition, determine if results of the TVRAs are available to the Cloud Service Provider.	√		√
9.3		**Third party agreement**			
9.3.3(a) Incremental	9.3.4(a)	ISO/IEC 27001:2005 does not cover all detailed attributes as stated in MTCS SS Requirement 9.3.3(a). Ensure that the contracts with third party service providers define appropriate clauses to address the relevant risks associated with the third parties.	√		
9.4		**Third party delivery management**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
9.4.4(a) New	9.4.4(a)	Verify that the Cloud Service Provider required third party service providers to implement policies, procedures and controls to protect confidentiality and security of sensitive information.	√		√
9.4.4(c) Incremental	9.4.4(c)	ISO/IEC 27001:2005 does not cover the establishment of a process to monitor the performance of the third party service provider. Check if the Cloud Service Providers are periodically monitoring the security practices and processes, covering all areas as listed in MTCS SS Requirement 9.4.4(c).	√		√
9.4.4(d) Incremental	9.4.4(d)	ISO/IEC 27001:2005 does not include the specific need for onsite visits. Verify that the onsite visits are conducted by the Cloud Service Provider and reports are produced for each visit.	√		√
9.4.4(e) Incremental	9.4.4(e)-(f)	ISO/IEC 27001:2005 does not cover the establishment of disaster recovery and contingency plans and procedures by third party service provider Check that the Cloud Service Provider has established a disaster recovery contingency framework with definition of roles and responsibilities for areas as listed in MTCS SS Requirement 9.4.4(e). Verify if the MTCS SS Audit Procedure 9.4.4(f), that defines controls to consider the worst case scenario for service interruption, is in place.	√		√
10		**Legal and compliance**			
10.2		**Compliance with policies and standards**			
10.2.4(a) Incremental	10.2.4(a)-(c)	ISO/IEC 27001:2005 does not include the specific frequencies for the various types of reviews. Verify that third party reviews and assessments shall be performed at least annually and the previously identified findings have been mitigated within the defined timeline.	√		√
10.3		**Prevention of misuse of cloud facilities**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
10.3.2(a)-(b) Incremental 10.3.2(c)-(d) New	10.3.4(a)	ISO/IEC 27001:2005 does not cover the enforcement of acceptable use policy regarding cloud specific requirements on the awareness of the cloud environment's permitted access and use, and the monitoring policies, procedures and tools in place. In addition, ISO/IEC 27001:2005 does not cover the configuration of log-on warning messages or reminder on access policies and monitoring for accessing infrastructure or other privileged access, and implementation of monitoring controls to detect if the cloud infrastructure is being used as a platform to attack others. Determine if the sufficiency of controls implemented to prevent the misuse of cloud facilities.	√	√	√
10.6		**Continuous compliance monitoring**			
10.6.4(a) New	10.6.4(a)	ISO/IEC 27001:2005 does not cover the provision of real-time monitoring for cloud users. Determine if cloud users have a platform to perform real-time monitoring of security controls.	√	√	√
11		**Incident management**			
11.1		**Information security incident response plan and procedures**			
11.1.4(a) Incremental	11.1.4(a) & (e)	ISO/IEC 27001:2005 does not cover the development of incident response plan and procedures. Determine if the Cloud Service Provider has established and documented an overall strategy in responding to threats as listed in MTCS SS Requirement 11.1.4(a). At minimum, the strategy should fulfil the requirements as listed in MTCS SS Requirement 11.1.4(a). Validate the efficiency of the incident response plan in mitigating risk during a simulated attack.	√		√

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
11.1.4(b) New	11.1.4(b)	ISO/IEC 27001:2005 does not cover the development of incident response plan and procedures. Determine if the Cloud Service Provider has sufficient plan to address public relation issues, as specified in MTCS SS Audit Procedure 11.1.4(b).	√		√
11.1.4(c) New	11.1.4(c)	ISO/IEC 27001:2005 does not cover the development of incident response plan and procedures. Verify that there is a mechanism to notify affected customers with details on incident, the impact and preventive measures.	√	√	√
11.2		**Information security incident response plan testing and updates**			
11.2.4(a) New	11.2.4(a)-(b)	ISO/IEC 27001:2005 does not cover the testing and updates of incident response plan. Check that the Cloud Service Provider conducted incident drills twice a year with defined components as stated in MTCS SS Requirement 11.2.4(a). Review the drills and determine if the lessons learnt from the drill have been incorporated into the plan.	√		√
11.4		**Problem management**			
11.4.3(a) Incremental	11.4.4(a)	ISO/IEC 27001:2005 does not cover the establishment of escalation processes for problems with different severity levels. Review the effectiveness of the problem management processes established by the Cloud Service Provider, as specified in MTCS SS Audit Procedure 11.4.4(a).	√		√
12		**Data Governance**			
12.1		**Data classification**			
12.1.3(c) Incremental	12.1.4(a)	ISO/IEC 27001:2005 does not specify the classification of communication channels. Determine if the communication channels have been classified.	√		
12.4		**Data labelling / handling**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.4.4(a) New	12.4.4(a)	ISO/IEC 27001:2005 does not cover the maintenance of logs and inventories of physical locations of cloud user data. Verify and review inventories of data and check the completeness of inventories including maintenance of logs and inventories of physical location of data.	√		√
12.4.4(b) Incremental	12.4.4(b)	While there are elements of media disposal in ISO/IEC 27001:2005, the specific requirement as stated in MTCS SS Requirement 12.4.4(b) is not covered. Review the documentation that defines controls on data handling upon termination.	√		
12.5		**Data protection**			
12.5.4(a) Incremental	12.5.4(a)	ISO/IEC 27001:2005 does not cover a data loss prevention strategy. Determine if Cloud Service Provider has established controls and procedures to protect data from loss and destruction as listed in MTCS SS Requirement 12.5.4(a).	√	√	√
12.6		**Data retention**			
12.6.4(a) New	12.6.4(a)	ISO/IEC 27001:2005 does not cover the provision of mechanisms for cloud users to remove or destroy all data themselves. Verify the effectiveness of controls implemented for cloud users to remove or destroy data in the event of contract termination (including backups) as defined in MTCS SS Audit Procedure 12.6.4(a).	√	√	√
12.7		**Data backups**			
12.7.2(b) Incremental	12.7.4(a)	ISO/IEC 27001:2005 does not cover the frequency of testing required on the backups. Ensure backups can be successfully restored as defined in MTCS SS Audit Procedure 12.7.4(a).			√
12.8		**Secure disposal and decommissioning of hardcopy, media and equipment**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.8.2(c) New	12.8.4(a)	ISO/IEC 27001:2005 does not cover the secure disposal and decommissioning procedures of hardcopy materials. Ensure the hardcopy materials have been disposed of properly by sampling some assets.			√
12.9		**Secure disposal verification of live instances and backups**			
12.9.3(a) Incremental	12.9.4(a)	ISO/IEC 27001:2005 does not include the requirement to verify that data has been securely removed. Verify the effectiveness of the deletion process by checking for any remains of the data that should have been securely deleted.		√	√
12.11		**Production data**			
12.11.3(a)-(d) Incremental	12.11.4(a)	ISO/IEC 27001:2005 does not cover tracking of production data for operational procedures and electronic commerce services. Determine if production data is residing in non-production systems by sampling the relevant systems.		√	√
13		**Audit logging and monitoring**			
13.1		**Logging and monitoring process**			
13.1.4(d) New	13.1.4(c) & (e)	Determine if the Cloud Service Provider has established a mechanism to follow up, verify and address all alerts in the system. Also, determine if the mechanism(s) established are appropriate and sufficient for its purpose.	√	√	√
13.2		**Log review**			
13.2.4(a) New	13.2.4(a)-(b)	Verify that the audit procedure, as defined in MTCS SS 13.2.4(a)-(b) has been implemented effectively.	√	√	√
13.3		**Audit Trails**			
13.3.3(a) Incremental	13.3.4(a)	ISO/IEC 27001:2005 does not specify the media to be used for capturing audit trails to prevent modifications. Assess the effectiveness of the controls implemented to protect audit trails from unauthorized modification or deletion from the media.		√	√
13.5		**Usage Logs**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
13.5.2(a) Incremental	13.5.4(a)	ISO/IEC 27001:2005 does not cover the protection of strict files and directories' permissions of usage logs. Determine the adequacy of the controls implemented to protect the usage log entries.		√	√
14		**Secure configuration**			
14.1		**Server and network device configuration standards**			
14.1.4(a) New	14.1.4(a)	ISO/IEC 27001:2005 does not cover the detailed components of the network security management and controls implementation stated in ISO/IEC 27001:2005 Clause A.10.6 and specification of industry accepted system hardening standards. As specified in MTCS SS Audit Procedure 14.1.4(a), review the documentation for systems and infrastructure to ensure the deployment of versions that meet EAL4 or comparable security assurance.	√		√
14.2		**Malicious code prevention**			
14.2.4(a) Incremental	14.2.4(a)	ISO/IEC 27001:2005 does not include the testing of prevention and detection capabilities present in the cloud infrastructure. As specified in MTCS SS Audit Procedure 14.2.4(a), verify that periodic testing of the prevention and detection capabilities and recovery procedures against malicious code is carried out by the Cloud Service Provider.	√		√
14.2.4(b) Incremental	14.2.4(b)	ISO/IEC 27001:2005 does not cover the sandboxing or isolation of any user provided code. Check that any user provided code is sandboxed or isolated to ensure the underlying platform and other tenants are not affected by the same code.	√	√	√
14.9		**Enforcement checks**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14.9.4(a) Incremental	14.9.4(a)-(b)	ISO/IEC 27001:2005 does not cover the specific frequency for compliance checks. Verify that compliance checks for security configurations are performed at least on a daily basis.	√		√
14.9.4(b) New	14.9.4(c)	ISO/IEC 27001:2005 does not cover the need for file integrity monitoring tools. Determine if file integrity monitoring tools have been implemented and are operating efficiently.	√	√	√
15		**Security testing and monitoring**			
15.1		**Vulnerability scanning**			
15.1.4(a) Incremental	15.1.4(a)-(b)	ISO/IEC 27001:2005 does not cover details of vulnerability (both internal and external) scanning as stated in MTCS SS Requirement 15.1.4. As stated in MTCS Audit Procedure 15.1.4(a)-(b), verify that internal and external vulnerability scanning is performed at least on a monthly basis, and the effectiveness of the scan, assessment and remediation are reviewed.	√		√
15.2		**Penetration testing**			
15.2.4(a) New	15.2.4(a)-(b)	Conducting of penetration testing at least twice annually, with at least one of the tests executed by a qualified third party. As stated in MTCS Audit Procedure 15.2.4(a)-(b), review the effectiveness of the penetration testing program including follow-up of identified findings.	√		√
15.3		**Security monitoring**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
15.3.4(a) Incremental	15.3.4(a)-(c)	ISO/IEC 27001:2005 does not include details pertaining to the depth and scope of the technical compliance reviews. Verify that the Cloud Service Provider includes the requirements as listed in MTCS SS 15.3.4(a) in its security monitoring process, which generally covers determining the frequency of technical compliance reviews on information systems, determining if technical depth and scope of review is sufficient, and determining if due diligence is observed in selecting personnel performing the reviews.	√		√
16		**System acquisitions and development**			
16.1		**Development, acquisition and release management**			
16.1.4(a) New	16.1.4(a)-(b)	Verify that the requirement specified in MTCS SS Clause 16.1.4 has been implemented.	√	√	√
16.2		**Web application security**			
16.2.4(a) New	16.2.4(a)	Check that the private / protected web services interfaces are included in web application testing.	√		√
16.4		**Source code security**			
16.4.2(a) Incremental	16.4.4(a)	ISO/IEC 27001:2005 does not cover version control. Determine the effective of the controls implemented to secure source code repositories.		√	√
17		**Encryption**			
17.1		**Encryption policies and procedures**			
17.1.2(a)-(b) Incremental	17.1.4(a)	Determine if the encryption policies and standards developed based on the requirements as stated in MTCS SS Clause 17.1.2 have been implemented and enforced effectively by the Cloud Service Provider.		√	√
17.2		**Channel encryption**			
17.2.2(a) Incremental	17.2.4(a)	ISO/IEC 27001:2005 does not cover specific usage of encryption. As specified in MTCS SS Audit Procedure 17.2.4(a), determine if non-encrypted access is available.		√	

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
17.3		**Key management**			
17.3.4(a) Incremental	17.3.4(a)	ISO/IEC 27001:2005 does not cover key management lifecycle process and controls. As specified in MTCS SS Audit Procedure 17.3.4(a), determine if the encryption keys are stored in tamper-resistant device such as hardware security modules of security assurance that comply with relevant agreements, laws and regulations.	√	√	√
18		**Physical and environmental**			
18.3		**Physical access**			
18.3.3(a) Incremental	18.3.4(a)	ISO/IEC 27001:2005 does not cover surveillance of access within data centre, and the monitoring and storage of access logs. As specified in MTCS SS Audit Procedure 18.3.4(a), review the effectiveness of the physical security controls and access logging present at the data centre.		√	√
19		**Operations**			
19.2		**Documentation of service operations and external dependencies**			
19.2.4(a) Incremental	19.2.4(a)	ISO/IEC 27001:2005 does not cover cloud specific documentations. Determine if documentation of all external dependencies is maintained by Cloud Service Provider.	√		√
19.3		**Capacity management**			
19.3.4(a) New	19.3.4(a)-(b)	ISO/IEC 27001:2005 does not cover tools for capacity monitoring. Check that the Cloud Service Provider put in place automated monitoring tools to continually monitor critical resources for capacity utilization (i.e., system or CPU, disk, memory, network bandwidth) and ensure that alert notification types and rules are appropriately set. Determine if the capacity management is effective at addressing risks to system uptime and performance.	√	√	√
19.4		**Service levels**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
19.4.4(a)-(f) Incremental	19.4.4(a)	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. Examine a sample of communications between Cloud Service Provider and cloud user on the components as listed in MTCS SS Clause 19.4.4(a)-(e) to determine the service level i.e., redundant network connectivity, minimum bandwidth, protection measures against malicious attacks, quality of service (QoS), bandwidth scalability on storage links, and any known limitation on the application / service.	√		√
19.5		**Reliability and resiliency**			
19.5.4(a) Incremental	19.5.4(a)-(b)	ISO/IEC 27001:2005 does not cover reliability and resiliency of storage systems. Determine whether a process exists to ensure reliability and resiliency of storage systems, which addresses the requirements as defined in MTCS SS Clause 19.5.4(a)-(h).	√	√	√
19.5.4(b)-(c) New					
19.5.4(d)-(f) Incremental					
19.5.4(g) New					
19.5.4(h) Incremental					
19.6		**Recoverability**			
19.6.3(a)-(b) Incremental	19.6.4(a)	ISO/IEC 2001:2005 does not cover details related to alternate sites and adequate point-in-time backup copies. Determine the effectiveness of the recoverability process of key infrastructure by reviewing the test results.		√	√
20		**Change management**			
20.3		**Back-out or rollback procedures**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
20.3.4(a) Incremental	20.3.4(a)	ISO/IEC 27001:2005 does not cover alternate recovery options. Determine if the Cloud Service Provider supports alternate recovery options to address situations where change is not successfully implemented in the production environment and there is a need to roll back to a former version.	√		√
20.5		**Patch management procedures**			
20.5.4(a) New	20.5.4(a)	Check that the Cloud Service Provider has established procedures to appropriately justify and track to closure, patches that were not applied.	√		√
21		**Business continuity planning (BCP) and disaster recovery (DR)**			
21.2		**BCP and DR plans**			
21.2.4(a) Incremental	21.2.4(a)	ISO/IEC 27001:2005 does not cover rapid operational and backup capabilities. Verify that rapid operational and backup capabilities are implemented at the individual system or application cluster level, and review if the risk assessments include criteria as listed in MTCS SS clause 21.2.4(a).	√	√	√
21.2.4(d) Incremental	21.2.4(c)	ISO/IEC 27001:2005 does not cover alternate recovery site. Verify that an alternate recovery site is geographically separated from the primary site to enable restoration of critical systems and resumption of business operations.	√		√
21.3		**BCP and DR testing**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
21.3.4(a) Incremental	21.3.4(a)-(b)	ISO/IEC 27001:2005 does not cover disaster recovery components. Check that business continuity and disaster recovery plans are tested and updated at least annually, and include plans for various test case scenarios (i.e., total shutdown or incapacitation of the primary site, component failure at the individual system or application cluster level, inter-dependencies between critical information assets, bilateral or multilateral recovery testing on networks and systems linked to specific third party service providers).	√		√
22		**Cloud services administration**			
22.6		**Password reset and first logon**			
22.6.4(a) Incremental	22.6.4(a)	ISO/IEC 27001:2005 does not cover details on password reset and change. Verify that half of the new password is with the user while the other half of the new password is with the user's supervisor.	√	√	√
22.7		**Administrator access security**			
22.7.4(a) Incremental	22.7.4(a)	ISO/IEC 27001:2005 does not cover privilege access management tools. Verify that privilege access management tools are implemented to restrict administrator's direct access to privileged functions and accounts.	√	√	√
22.9.4		**Session Management**			
22.9.2(b) Incremental	22.9.4(a)	Review the effectiveness of the session management controls in use to fulfil requirements as stated in MTCS SS Clause 22.9.2(b).		√	
22.1		**Segregation of duties**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.10.4(a) Incremental	22.10.4(a)-(b)	ISO/IEC 27001:2005 does not specify the frequency for user access rights and the segregation of duties reviews As specified in MTCS SS Audit Procedure 22.10.4(a)-(b) check that the Cloud Service Provider has conducted monthly reviewed access rights and segregation of duties. Assess controls for segregation of duty to determine if they are adequate for the risks faced by the Cloud Service Provider.	√		
22.11		**Secure transmission of access credentials**			
22.11.2(a) New	22.11.4(a)	As specified in MTCS SS Audit Procedure 22.11.4(a), identify clear text credentials in transit for administrative access by reviewing a sample of network traffic.		√	
22.12		**Third party administrative access**			
22.12.4(a) Incremental	22.12.4(a)	ISO/IEC 27001:2005 does not cover the granting of access to vendors. As specified in MTCS SS Audit Procedure 22.12.4(a), verify that third party access to the environment is only allowed under the direct supervision of the Cloud Service Provider's relevant personnel.	√		√
22.13		**Service and application accounts**			
22.13.4(a) Incremental	22.13.4(a)-(b)	ISO/IEC 27001:2005 does not cover service and application accounts. Verify that the Cloud Service Provider has established procedures to change service account passwords in accordance with the requirement stated in MTCS SS Clause 22.13.4(a).	√		
23		**Cloud user access**			
23.2		**User access security**			
23.2.4(a) New	23.2.4(a)	Verify if the requirement on federated identity management, as stated in MTCS SS Clause 23.2.4(a) has been implemented.	√	√	√
23.6		**Password Protection**			

MTCS SS Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.6.2(a)-(b) Incremental 23.6.2(c) New	23.6.4(a)	Determine if passwords are adequately protected in accordance with requirements as stated in MTCS SS Clause 23.6.2(a)-(c) by reviewing a sample of passwords in transit and storage.		√	√
24		**Tenancy and customer isolation**			
24.1		**Multi tenancy**			
24.1.4(a)-(c) New	24.1.4(a)	ISO/IEC 27001:2005 does not cover multi tenancy and segregation between virtual machines belonging to different users. Verify that monitoring and blocking mechanisms are implemented in accordance MTCS SS Clause 24.1.4(a)-(c).	√	√	√
24.5		**Storage area networks (SANs)**			
24.5.4(a)-(b) New 24.5.4(d) New	24.5.4(a)	ISO/IEC 27001:2005 does not cover equipment security for SANs. Review the SANs configuration to ensure that it includes the requirements as specified in MTCS SS Clause 24.5.4(a)-(b) and 24.5.4(d).	√	√	√
24.6		**Data segregation**			
24.6.4(a) Incremental	24.6.4(a)	ISO/IEC 27001:2005 does not cover cloud user control over encryption keys. Determine if encryption keys can be controlled in accordance with the requirements specified in MTCS SS Clause 24.6.4(a).	√	√	√
24.6.4(b) New	24.6.4(b)	ISO/IEC 27001:2005 does not include logical segregation for backups. Determine if backups are segregated in accordance with the requirements specified in MTCS SS Clause 24.6.4(b).			

<End of Audit Checklist Report>