INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

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

For cross-certification from Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) to MTCS SS

December 2014

Revision History

Revision Date	Version	Updated by	Description
December 2014	Version 1.0	IDA	Initial Release

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 CSA STAR 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
Aloysius Cheang	Cloud Security Alliance APAC
Daniele Catteddu	Cloud Security Alliance EMEA

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

Contents

1 Normative References

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

- **Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS).** MTCS SS aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS SS provides relevant cloud computing security practices and controls for cloud users, auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers to strengthen and demonstrate the cloud security controls in their cloud environments.
- **CSA Cloud Control Matrix (CCM) v3.0.** The Cloud Security Alliance (CSA) launched the Security, Trust & Assurance Registry (STAR) initiative at the end of 2011, in order to improve security posture in the cloud. CSA CCM v3.0 was defined to support this framework. It provides the guidance on necessary security controls for a Cloud Service Provider to assess the maturity of their security framework.
- **ISO/IEC 27001:2013** *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 27001:2013 Standard is the second edition of the standard and replaces the first edition ISO/IEC 27001:2005 Standard. This standard benefits entities in allowing them to demonstrate commitment and compliance via the adoption of this standard.

2 Purpose of Document

This Audit Checklist Report is the third report in the set of three (3) documents to support cross-certification between MTCS SS and CSA STAR (Note that CSA STAR is based on CCM v3.0 and ISO/IEC 27001:2013). The purpose of each document is described in the diagram below.

This Audit Checklist Report and associated audit procedures are intended to help CSA STAR certified Cloud Service Providers in performing a trial cross-certification with auditors / certification bodies on MTCS SS. As such, this document does not include audit related information on recommended audit timeline and competency criteria for auditors.

Note that this document only covers gaps identified in the 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 CSA STAR. The information provided in this document aims to assist entities that are CSA STAR certified to adopt MTCS SS. Cloud Service Providers that are CSA STAR certified will have to comply with the requirements stated in MTCS SS that are not fully covered in CSA STAR.	The purpose of the Implementation Guideline Report is to assist Cloud Service Providers that are CSA STAR certified to implement MTCS SS. The guidelines in the report are generic and need to be tailored to each Cloud Service Provider's specific requirements.	The purpose of the Audit Checklist Report is to guide auditors, including internal audit function, MTCS SS certification bodies and external audit bodies in understanding additional requirements beyond CSA STAR. From the Cloud Service Providers' perspective, this document serves as a general guide for them to understand the scope covered in MTCS SS certification audit when the scope of the CSA STAR audit overlaps with scope of MTCS SS.

3 Intended Audience

This Audit Checklist Report is intended for Cloud Service Providers that are CSA STAR certified and interested in obtaining certification for MTCS SS Levels 1, 2 or 3.

This report is also intended to guide auditors, including internal auditors, MTCS SS certification bodies and external audit bodies on the differences between MTCS SS and CSA STAR, and the required audit procedures.

4 Scope

The Audit Checklist Report includes the gaps identified in the Gap Analysis Report, which are classified as "INCREMENTAL" or "NEW". For ease of reference, the description of the gap classifications is listed below. For the full report on the gap analysis, refer to the Gap Analysis Report.

Gap Classification	Description
INCREMENTAL	Indicates the clauses in MTCS SS that are stated with more details than the corresponding sections in clauses in CSA STAR[1]. In general, the requirements are classified as "INCREMENTAL" if the required enhancements on the existing CSA STAR[1] characteristics are not costly or onerous in nature.
NEW	Indicates the clauses in MTCS SS that are absent, or stated with significantly more detail than the corresponding sections and clauses in CSA STAR[1]. In general, the requirements are classified as "NEW" if there may be a material financial cost to meet relevant MTCS SS requirement, additional controls to be included in the audit checklist and / or the effort is relatively onerous.

[1]CSA STAR includes clauses in CSA CCM v3.0 and ISO/IEC 27001:2013.

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

Gap Classification	Description
INCLUDED	Indicates the clause in MTCS SS that are equally represented in CSA STAR[1]

[1]CSA STAR includes clauses in CSA CCM v3.0 and ISO/IEC 27001:2013.

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

Cloud-related terms used in this report are defined in CSA CCM v3.0, MTCS SS and ISO/IEC 27001:2013.

7 Tips on Using this Audit Checklist Report

Section 8 includes the corresponding audit procedures required for gaps identified in the Gap Analysis Report. This list is intended to guide auditors and Cloud Service Providers certified in CSA STAR 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 them to understand the incremental scope covered in MTCS SS certification audits when already CSA STAR 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 auditors and MTCS SS external auditors.

It is recommended for Cloud Service Providers to refer to the Implementation Guideline Report while using this document. 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 / Visual Control 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 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 SS 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 implemented 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 controls 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 CSA CCM. Identified gaps between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 are highlighted in the Gap Analysis Report and these clauses are not included in this report.

MTCS Clause / 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(j) Incremental	6.1.2 (a)	CSA CCM does not cover specific details related to risk mitigation. Determine if the technical and / or procedural controls, associated with the following areas have been implemented as part of ISMS: • mitigate risk from authorised insiders; and • manage virtualisation security for cloud services.	√	√	
6.5 Review of information security policy					
6.5.2(a) Incremental	6.5.2(a)-(d)	CSA CCM does not specifically require an annual review of the information security policy. Determine if the Cloud Service Provider's Information Security Policy has been reviewed, at least on an annual basis.	√		
6.6 Information security audits					
6.6.2(a)-(b) Incremental	6.6.2(a)-(b)	CSA CCM does not cover the establishment of an audit committee and the approval of IT security audit plans by a formal 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). Determine if IT security audit plans have been approved by the audit committee formed as per MTCS SS Requirement 6.6.2(a).	√		
8 Risk management					
8.2 Risk assessment					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
8.2.2(b) Incremental	8.2.2(c)	CSA CCM does not specifically require risk assessments to include risks relating to those as stated in MTCS SS. Verify that the risk assessments are conducted in sufficient detail and cover the risk categories as stated in MTCS SS Requirement 8.2.2(b).	√		
10 Legal and compliance					
10.3 Prevention of misuse of cloud facilities					
10.3.2(b), (d) Incremental	10.3.2(a)	CSA CCM does not cover specific requirements on the prevention of cloud facilities misuse. Determine if the following controls have been implemented: • training sessions pertaining to the monitoring policies, procedures and tools in place have been conducted ; • monitoring to detect if the cloud infrastructure is being used as a platform to attack others and • agreements to include coverage of access and monitoring policies and controls.	√	√	
10.6 Continuous compliance monitoring					
10.6.2(a) Incremental	10.6.2(a)	CSA CCM does not cover the provision of continuous or real-time compliance monitoring. Verify if a system configuration compliance reporting framework is implemented for areas as stated in MTCS SS Requirement 10.6.2(a).	√	√	
11 Incident management					
11.2 Information security incident response plan testing and updates					
11.2.2(b) Incremental	11.2.2(a)-(b)	CSA CCM does not cover details relevant to information security incident response plan testing. Determine if the following controls are in place: • details on types of tests, scope of tests and parties to be involved in the test execution and review have been included in the incident response test plan; • information security incident response plan is tested on an annual basis; and • appropriate training has been conducted for relevant personnel.	√	√	√

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12 Data governance					
12.5 Data protection					
12.5.2(a) Incremental	12.5.2(a)	CSA CCM does not cover specific media handling processes for virtualised images and snapshots. Determine if sufficient security controls have been implemented on the access to all media, virtualised images and snapshots to protect data from loss and destruction.	√	√	
12.7 Data backups					
12.7.2(a) Incremental	12.7.2(a)	CSA CCM does not specify controls for the encryption of backups stored off-site. Determine if the appropriate cryptographic controls are in place to protect backups before they are transported to be stored off-site.	√	√	
12.7.2(c) Incremental	12.7.2(d)	CSA CCM does not cover controls related to 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					
12.8.2(c) Incremental	12.8.2(d)	CSA CCM does not specifically cover the secure disposal and decommissioning procedures of hardcopy materials. Determine if the Cloud Service Provider has established secure disposal procedures for hardcopy materials, media and equipment, which include methods as stated in MTCS SS Requirement 12.8.2(c), so that data cannot be reconstructed. Alternatively, verify if the Cloud Service Provider has obtained a “Certificate of Destruction” from a data disposal third party as evidence of secure disposal.	√	√	
14 Secure configuration					
14.1 Server and network device configuration standards					
14.1.2(b), (d), (e) Incremental	14.1.2(a)-(c)	CSA CCM does not cover specific requirements on system components and network devices in its configuration standards requirements. Refer to MTCS SS Requirements 14.1.2(b)-(e) for specific requirements regarding server and network device configuration standards and validate if they have been implemented.	√	√	

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14.2 Malicious code prevention					
14.2.2(e) Incremental	14.2.2(c)-(f)	CSA CCM does not cover specific control requirements for malicious code prevention. Refer to MTCS SS Audit Procedures 14.2.2(c)-(f) for specific audit procedures regarding malicious code prevention.	√	√	
15 Security testing and monitoring					
15.1 Vulnerability scanning					
15.1.2(a)-(b) Incremental	15.1.2(a)-(b)	CSA CCM requires vulnerability scanning to be performed at least on an annual basis. Determine if the following requirements with regards to vulnerability scanning have been performed: • quarterly scanning for vulnerabilities; and • vulnerabilities with a Common Vulnerability Scoring System (CVSS) base score of 7-10, or similar identified vulnerabilities are addressed, within a week.	√		
15.2 Penetration testing					
15.2.2(a) Incremental	15.2.2(a)	CSA CCM does not specify the required frequency for conducting penetration tests. Determine if the network layer and application layer penetration testing from locations as specified in MTCS SS Requirement 15.2.1 have been conducted by the Cloud Service Provider at least on an annual basis. In addition, determine if output of these tests and relevant follow-up actions have been maintained by the Cloud Service Provider.	√		
16 System acquisitions and development					
16.1 Development, acquisition and release management					
16.1.2(b), (j)-(k) Incremental	16.1.2(a)-(g)	While CSA CCM requires applications to be developed as per industry standards, it does not include additional details that are relevant to the development and acquisition of components as stated in MTCS SS	√	√	

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
		Requirement 16.1.2. Determine if the Cloud Service Provider has removed components as stated in stated in MTCS SS Requirements 16.1.2(b) and 16.1.2(c) before the production systems become active. In addition, determine if the Cloud Service Provider has used static code analysis tools against all source codes and that all source codes have been established as being authentic.			
17 Encryption					
17.3 Key management					
17.3.2(d) Incremental	17.3.2(a)-(b)	CSA CCM does not specifically require the formal acknowledgement of responsibilities from cryptographic key custodians. Determine if the Cloud Service Provider require cryptographic key custodians to formally and explicitly acknowledge their responsibilities as key custodians.	√		
17.4 Electronic messaging security					
17.4.2(c)-(f) Incremental	17.4.2(a)-(d)	CSA CCM does not cover the details on electronic messaging security as stated in MTCS SS Requirements 17.4.2(a)-(f). Determine if the following controls are in place: • Sufficient protection mechanisms to protect messages from unauthorised access, modification or diversion. • 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.	√	√	

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
18 Physical and environmental					
18.4 Visitors					
18.4.2(a)-(d) Incremental	18.4.2(a)-(c),(e)	CSA CCM does not specify the security controls to address security related to visitors. Determine if the Cloud Service Provider has established the following procedures to address security risks associated with visitors: • have authorised visitors be escorted by authorised personnel; • differentiate visitors and on-site personnel using identification pass or badge; • maintain a visitor log; and • review the above-mentioned visitor log periodically.		√	
18.6 Physical security review					
18.6.2(b) Incremental	18.6.2(a)	CSA CCM does not specifically require the periodical review of the organisation's physical security. Determine if reviews have been conducted by the Cloud Service Provider for its physical security at least on an annual basis.	√		
20 Change management					
20.5 Patch management procedures					
20.5.2(b) Incremental	20.5.2(a)	CSA CCM does not cover procedures on patch management for dormant / offline systems. Determine if appropriate patch management procedures have been established by the Cloud Service Provider for systems that have been dormant / offline for a period of time. In addition, determine if the procedures have been kept updated and relevant.	√	√	
22 Cloud services administration					
22.2 Generation of administrator passwords					
22.2.2(c) Incremental	22.2.2(a)-(b)	CSA CCM does not cover specific details on administrator passwords. Determine if the following requirements, as defined in MTCS SS	√	√	

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
		Requirements 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					
22.3.2(c) Incremental	22.3.2(c)	While CSA CCM covers the account management controls in general, the specific frequency to perform such review is not mentioned. Determine if formal access review and revocation processes have been established to ensure review is performed at least every ninety (90) days and notify the relevant parties of the action taken above.		√	
22.4 Account lockout					
22.4.2(a)-(b) Incremental	22.4.2(a)-(b)	While CSA CCM covers user access controls in general, specific requirements as stated in MTCS SS Requirement 22.4.2 are not mentioned. Determine if a formal process to detect and terminate unauthorised access attempts in a timely manner has been implemented by the Cloud Service Provider. In addition, verify that account lockout requirements have been established based on the risk assessments and sensitivity of the system and data.		√	
22.5 Password change					
22.5.2(b) Incremental	22.5.2(a)-(b)	While CSA CCM covers some elements of password change, details as stated in MTCS SS Requirement 22.5.2 are not included. Determine if the Cloud Service Provider enforces compulsory password change based on the industry standard practices and if passwords satisfy the requirement as stated in MTCS SS Requirement 22.5.2(b).		√	
22.6 Password reset and first logon					
22.6.2(a)-(d) Incremental	22.6.2(a)	CSA CCM does not cover details on password reset and change, and two-factor authentication (2FA). Determine if the Cloud Service Provider has configurations in place to:	√	√	

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
		• ensure generation of unique passwords; • require users to verify their identify in the event of a password change; • obtain management approval for a password reset; and • reset the password in the event of a lost 2-factor authentication device.			
22.7 Administrator access security					
22.7.2(a) Incremental	22.7.2(a)-(b)	CSA CCM does not explicitly require access to be restricted to the Cloud Service Management Network and Cloud Service Delivery Network. Determine if configurations are in place to only allow access from the Cloud Service Provider Internal Network to the Cloud Service Management Network and Cloud Service Delivery Network from specific IP addresses or network segments.	√	√	
22.7.2(e) Incremental	22.7.2(d)	Determine if policies and configurations are in place to: • restrict the use of local administrative accounts; • require explicit approval for the enabling and usage of administrative access; and • manage administrative access through role-based access control mechanisms.	√	√	
22.9 Session management					
22.9.2(b) Incremental	22.9.2(a)-(c)	CSA CCM does not specifically cover the details on the reactivation of idle sessions. Determine if the Cloud Service Provider has configuration in place to re-enter passwords to reactivate terminals after session idle time of more than 15 minutes.	√	√	
22.10 Segregation of duties					
22.10.2(a) Incremental	22.10.2(a)	While CSA CCM covers the review of user access rights and the segregation of duties in general, the specific frequency of such reviews is not included. Determine if the Cloud Service Provider has reviewed access rights and segregation of duties at least on an annual basis.	√	√	
22.13 Service and application accounts					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.13.2(a) Incremental	22.13.2(a)-(d)	CSA CCM does not cover the details on service and application accounts. Determine if the Cloud Service Provider has all service and application accounts created in accordance with the requirements as stated in MTCS SS Requirement 22.13.2(a).	√	√	
23 Cloud user access					
23.2 User access security					
23.2.2(c)-(e) Incremental	23.2.2(a)-(e)	CSA CCM does not cover the details on documented approval processes, having a default “deny all” setting and having anti-bot controls in place. Determine if the Cloud Service Provider has the following in place: • 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(c) Incremental	23.3.2(a)-(b)	While CSA CCM covers password controls for mobile devices and wireless, specific password criteria as stated in MTCS SS Requirement 23.3.2(a) are not mentioned. Determine if the Cloud Service Provider has policies and configurations in place to address the minimum password criteria as stated in MTCS SS Requirement 23.3.2(a), and generic and shared passwords with other accounts have been disallowed.		√	
23.4 User account lockout					
23.4.2(a)-(b) Incremental	23.4.2(a)-(b)	CSA CCM does not cover details on account lockout. The Cloud Service Provider shall implement configuration or measures to lock out user accounts based on the criteria as stated in MTCS SS Requirement 23.4.2. Reviews shall also be conducted by the Cloud Service Provider to ensure that configurations have been implemented in accordance with the hardening documents approved beforehand.		√	
23.5 User password reset and 1st logon change					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.5.2(b) incremental	23.5.2(a)-(b)	CSA CCM does not cover details on first time logons. Determine if the Cloud Service Provider has policies and configurations in place that require users to verify their identity before password reset is processed.	√	√	
23.6 Password protection					
23.6.2(a)-(c) Incremental	23.6.2(a)-(b)	While CSA CCM covers access control requirements in general, specific controls as stated in MTCS SS Requirement 23.6.2 are not included. Determine if the Cloud Service Provider has password controls in place as stated in MTCS SS Requirement 23.6.2.		√	
23.7 User session management					
23.7.2(a)-(c) Incremental	23.7.2(a)-(b)	While CSA CCM covers access control requirements in general, specific controls as stated in MTCS SS Requirement 23.7.2 are not included. Determine if the Cloud Service Provider has configurations in place to: • deactivate user sessions after a period of inactivity; • require users to re-enter passwords to reactivate terminals that have been idle for more than fifteen (15) minutes; and • implement cryptographically strong identifiers for each user session.		√	
23.9 Self-service portal creation and management of user accounts					
23.9.2(a) Incremental	23.9.2(a)	CSA CCM does not cover specific password criteria for self-service portals. Determine if the Cloud Service Provider has maintained strict password criteria in accordance with requirements defined in MTCS SS Requirement 23.3.		√	
23.10 Communication with cloud users					
23.10.2(a) Incremental	23.10.2(a)	CSA CCM does not cover the availability of a secure distribution channel for official notifications. Determine if the Cloud Service Provider has implemented appropriate communication mechanisms to communicate official notifications securely to cloud users.		√	
24 Tenancy and customer isolation					
24.3 Network protection					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
24.3.2(m) Incremental	24.3.2(g)	CSA CCM does not specifically require that any traffic from the wireless network be denied access to the cloud infrastructure networks and cloud service management networks. Determine if the Cloud Service Provider has configured their network firewalls to deny any traffic from the wireless environment to critical cloud infrastructure and management networks.	√	√	
24.4 Virtualisation					
24.4.2(a) Incremental 24.4.2(c) Incremental	24.4.2(a)-(b)	While CSA CCM covers virtualisation security in general, it does not include details as mentioned in MTCS SS Requirements 24.4.2(a) and 24.4.2(c). Determine if the Cloud Service Provider has identified security risks including, but not limited to, those as stated in MTCS SS Requirement 24.4.2(a), and appropriately addressed them. In addition, determine if the Cloud Service Provider has encrypted the virtual machines to protect them against theft.	√	√	
24.5 Storage area networks (SANs)					
24.5.2(a)-(b) Incremental	24.5.2(a)-(b)	CSA CCM does not cover equipment security specifically for SANs. Determine if the Cloud Service Provider has access controls in place to limit the devices that can communicate with network attached storage devices and has established processes or procedures to ensure that changes to SANs and associated network components are correctly and accurately propagated.	√	√	

8.2 MTCS SS Level 2

This section summarises the audit guidance for gaps identified between MTCS SS Level 2 and CSA STAR. Identified gaps between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 are highlighted in the Gap Analysis Report and these clauses are not included in this report.

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6 Information security management					
6.5 Review of information security policy					
6.5.3(a) Incremental	6.5.3(a)-(d)	CSA CCM does not specifically require the review of the information security policy to be conducted at least twice in a year. Determine if the Cloud Service Provider has reviewed the Information Security Policy at least twice in a year.	√		
6.6 Information security audits					
6.6.2(a)-(b) Incremental	6.6.3(a)	CSA CCM does not cover the establishment of an audit committee and the approval of IT security audit plans by a formal 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). Determine if IT security audit plans have been approved by the audit committee formed as per MTCS SS Requirement 6.6.2(a). Determine how well the audit staffs understand the risks faced by the organisation by conducting interviews with relevant personnel.	√		√
7 Human resources					
7.1 Background screening					
7.1.3(a) Incremental	7.1.3(a)	CSA CCM does not specifically require background checks for personnel with access to critical cloud infrastructure networks to be performed at specific frequencies. Determine if background checks have been performed on personnel with access to the Cloud Service Management Network or Cloud Service Delivery Network at least annually.	√		
7.2 Continuous personnel evaluation					
7.2.3(a)-(b) New	7.2.3(a)-(b)	CSA CCM does not cover the frequency of continuous personnel evaluation. Determine if annual continuous evaluation has been	√		

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
		conducted for personnel with access to the Cloud Service Management Network or Cloud Service Delivery Network. Also, determine if the evaluation conducted covered at minimum the areas as stated in MTCS SS Requirement 7.2.3(b).			
8 Risk management					
8.4 Risk register					
8.4.3(a) Incremental	8.4.3(a)-(b)	CSA CCM does not specifically require the establishment of a risk register containing the risk attributes stated in the MTCS SS Requirement 8.4.3(a) for risk management. Determine if the Cloud Service Provider has established a risk register defining the abovementioned risk attributes in the risk management process.	√		
10 Legal and compliance					
10.3 Prevention of misuse of cloud facilities					
10.3.2(b), (d) Incremental	10.3.3(a)	CSA CCM does not cover in detail the requirements on the prevention of misuse of cloud facilities. Determine if the following controls have been implemented: • training sessions pertaining to the monitoring policies, procedures and tools in place have been conducted; • monitoring to detect if the cloud infrastructure is being used as a platform to attack others; and • the inclusion of access and monitoring policies / restrictions in third party contracts and agreements. Determine if employees understand what is prohibited or disallowed with regards to the misuse of cloud facilities by interviewing a sample of these employees.	√	√	
10.6 Continuous compliance monitoring					
10.6.3(a) Incremental	10.6.3(a)	CSA CCM does not cover the reporting requirements for system access. Determine if 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.	√		

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12 Data governance					
12.6 Data retention					
12.6.3(d) Incremental	12.6.3(c)	While CSA CCM requires retention controls to be in place, it does not specify the mechanisms and rules. Determine if the Cloud Service Provider has implemented periodic manual or automatic processes to identify and delete all data exceeding the retention period defined.	√	√	
12.8 Secure disposal and decommissioning of hardcopy, media and equipment					
12.8.2(c) Incremental	12.8.3(a)	CSA CCM does not specifically cover the secure disposal and decommissioning procedures of hardcopy materials. Determine if the Cloud Service Provider has established secure disposal procedures for hardcopy materials, media and equipment, which include methods as stated in MTCS SS Requirement 12.8.2(c), so that data cannot be reconstructed. Alternatively, verify if the cloud service provider has obtained a "Certificate of Destruction" from a data disposal third party as evidence of secure disposal. In addition, determine if relevant personnel are aware of and understands the disposal procedures by interviewing a sample of these personnel.	√		
13 Audit logging and monitoring					
13.2 Log review					
13.2.3(a) Incremental	13.2.3(a)-(d)	CSA CCM does not require log reviews to be performed for all critical systems and services performing security functions. Determine if the Cloud Service Provider has performed log reviews for all system components as stated in MTCS SS Requirement 13.2.3(a) at least on a daily basis.	√	√	
13.4 Backup and retention of audit trails					
13.4.3(b) Incremental	13.4.3(c)-(d)	CSA CCM does not specify additional details with regard to logs that are accessible via the internet. Determine if the Cloud Service Provider has implemented configurations such that logs that are accessible via the internet will be written onto a log server located on an internal network segment protected by a firewall. In addition, determine if the Cloud Service Provider has disallowed remote access to the log server and is only allowing local access via tightly controlled user IDs.	√	√	
14 Secure configuration					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14.9 Enforcement checks					
14.9.3(a) Incremental	14.9.3(a)-(b)	Determine if the Cloud Service Provider is performing checks on its security configurations at least on a weekly basis.	√		
15 Security testing and monitoring					
15.1 Vulnerability scanning					
15.1.3(a) Incremental	15.1.3(a)	Determine if the Cloud Service Provider is conducting vulnerability scanning at least on a quarterly basis and when significant changes occur to the environment.	√		√
15.1.3(b) Incremental	15.1.3(b)	CSA CCM does not require the usage of the Common Vulnerability Scoring System (CVSS) to address vulnerabilities timely. Determine if the Cloud Service Provider is addressing vulnerabilities with a CVSS base score of 4-6.9, or similar scoring mechanism, within one month.		√	
16 System acquisitions and development					
16.1 Development, acquisition and release management					
16.1.3(a) Incremental	16.1.3(a)-(b)	CSA CCM does not cover the verification of the integrity and authenticity of the applications. Determine if protection controls that allow the clients to verify the integrity and authenticity of the applications have been implemented. In addition, examine that proper test cases have been developed and changes / new development of a system have been signed off. Determine if developers understand secure coding practices.	√	√	√
16.2 Web application security					
16.2.3(a) Incremental	16.2.3(a)	CSA CCM does not specifically require the use of vulnerability security assessment tools or mechanisms. Determine if the Cloud Service Provider is reviewing public-facing web applications using manual or automated application vulnerability security assessment tools or mechanisms at least on an annual basis or when changes are made to the applications. In addition, determine if these reviews include, at the minimum, the identification of common web application vulnerabilities such as the OWASP Top Ten.	√		
16.2.3(c) Incremental	16.2.3(a)	CSA CCM does not require the security testing of public web services. Determine if the Cloud Service Provider is including public web services in security testing processes as per MTCS SS Requirement 16.2.3(a).	√		

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
17 Encryption					
17.3 Key management					
17.3.3(c) New	17.3.3(d)	CSA CCM does not cover specific key management lifecycle process and controls. Determine if specific requirements in MTCS SS Requirement 17.3.3 have been implemented by the Cloud Service Provider.	√	√	
17.3.3(d)-(e) Incremental	17.3.3(e)		√	√	
17.3.3(f)-(h) Incremental	17.3.3(f)		√	√	
18 Physical and environmental					
18.3 Physical access					
18.3.3(a) Incremental	18.3.3(a)-(c)	Determine if the Cloud Service Provider is monitoring individual access to areas hosting sensitive data and store access logs for at least three (3) months. Cloud Service Providers that adopt access card security or similar control to monitor individual access to such areas can review the access logs generated by the relevant systems.	√	√	
18.4 Visitors					
18.4.3(a) New	18.4.3(a)	CSA CCM does not include management approval as part of access control policy. Determine if the Cloud Service Provider has established that management approval is a prerequisite before visitors are allowed into facilities where sensitive data is hosted.	√	√	
20 Change management					
20.3 Back-out or rollback procedures					

MTCS Clause / 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)	CSA CCM does not cover rollback plans and procedures as part of backup management. Determine if the Cloud Service Provider has established a procedure to rollback to a former version if problem is encountered during or after the deployment of changes. If required, 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(c) Incremental	20.5.3(d)	CSA CCM does not require the testing of patches. Determine if the Cloud Service Provider has tested patches in a test environment mirroring the production environment prior to applying them.	√		
20.5.3(d) Incremental	20.5.3(b)-(c)	CSA CCM does not cover hardening of dormant or offline systems. Determine if the Cloud Service Provider has implemented a process to ensure that systems dormant or offline for over thirty (30) days are configured to meet hardening standards and all security software including patches is up to date. See TR 30:2012 Technical Reference for Virtualisation Security for servers Clause 8.5 Risk #4 – Security of dormant or offline VMs for additional details.	√	√	
21 Business continuity planning (BCP) and disaster recovery (DR)					
21.1 BCP framework					
21.1.3(b) Incremental	21.1.3(a)	Determine if the Cloud Service Provider has defined Recovery Point Objective (RPO) for each of their service offerings.	√		
22 Cloud services administration					
22.2 Generation of administrator passwords					
22.2.3(a) Incremental	22.2.3(a)	CSA CCM requires password policies to be documented and enforced but it does not include specific password criteria. Determine if the Cloud Service Provider has implemented minimum password criteria as stated in MTCS SS Requirement 22.2.3(a). If the Cloud Service Provider has implemented other solutions, determine if the alternative solution implemented can provide equivalent or better security.	√	√	
22.4 Account lockout					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.4.3(a) Incremental	22.4.3(a)-(c)	CSA CCM does not cover details about account lockout. Determine if the Cloud Service Provider has implemented configurations to only allow unlocks by administrators manually.		√	
22.6 Password reset and first logon					
22.6.3(a) Incremental	22.6.3(a)	CSA CCM covers password management in general but not the splitting of password. Determine if the Cloud Service Provider has implemented controls to ensure that the new password provided is split controlled and via out-of-band mechanism such that no one user has knowledge of the whole password in transit.	√		
22.7 Administrator access security					
22.7.3(a) New	22.7.3(a)-(b)	CSA CCM does not cover bastion hosts. Determine if access from network locations as stated in MTCS SS Requirement 22.7.3 is only permitted via bastion hosts.	√	√	
22.9 Session management					
22.9.2(a) Incremental	22.9.3(a)	CSA CCM does not specifically cover details about reactivation of idle sessions. Determine if the Cloud Service Provider has configurations in place to require the re-entering of passwords to reactivate terminals after session idle time of more than fifteen (15) minutes.	√	√	
22.10 Segregation of duties					
22.10.3(a) Incremental	22.10.3(a)	Determine if the Cloud Service Provider has conducted reviews of access rights and segregation of duties at least on a quarterly basis.	√		
22.13 Service and application accounts					
22.13.3(a)-(c), (e) Incremental	22.13.3(a)-(b)	ISO/IEC 27001:2005 does not cover detailed requirements pertaining to service and application accounts. Determine if the Cloud Service Provider has addressed all requirements as stated in MTCS SS Requirement 22.13.3.	√	√	
23 Cloud user access					
23.3 User access password					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.3.3(a) Incremental	23.3.3(a)	CSA CCM does not define specific criteria for passwords. Determine if the Cloud Service Provider has implemented minimum password criteria as stated in MTCS SS Requirement 23.3.3(a). If other solutions have been implemented, determine if the alternative solution provides equivalent or better security.		√	
23.4 User account lockout					
23.4.3(a)-(b) Incremental	23.4.3(a)-(b)	CSA CCM does not cover details pertaining to account lockout. Determine if the Cloud Service Provider has implemented configurations to lock out a user ID after a maximum of six (6) unsuccessful login attempts and only allow administrators to enable the user ID.		√	
23.6 Password protection					
23.6.2(a)-(c) Incremental	23.6.3(a)	While CSA CCM covers access control requirements in general, specific controls as stated in MTCS SS Requirement 23.6.2 are not included. Determine if the Cloud Service Provider has controls in place to ensure that all passwords are rendered unreadable during transmission, and channels where the transmission is performed and the password storage is encrypted. Verify the level of knowledge of relevant administrators and developers on password protection requirements by interviewing a sample of these administrators and developers.	√		
23.8 Change of cloud user's administrator details notification					
23.8.3(a)-(b) Incremental	23.8.3(a)-(b)	CSA CCM does not cover the alert for any change in administrator details and approval being needed for changing the cloud user's administrator details. Determine if the Cloud Service Provider has appropriate procedural or technical measures in place to ensure that a change in the cloud user's administrator details trigger an alert to the administrator and the change will only be effected after the Cloud Service Provider's administrator approves the change.		√	
23.10 Communication with cloud users					
23.10.3(a) Incremental	23.10.3(a)	CSA CCM does not specify topics for user education. Determine if the Cloud Service Provider is providing user education on topics including, but not limited to, those as stated in MTCS SS Requirement 23.10.3(a).	√		
24 Tenancy and customer isolation					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
24.2 Supporting infrastructure segmentation					
24.2.3(a) Incremental	24.2.3(a)	While CSA CCM covers network security in general, it does not include the separation of authentication sources. Determine if the Cloud Service Provider has configurations in place to separate authentication sources for network locations as stated in MTCS SS Requirement 24.2.3(a).	√	√	
24.2.3(b)-(c) Incremental	24.2.3(b)-(c)	CSA CCM does not specifically require that direct access be disallowed to the Cloud Service Delivery Networks and Cloud Service Provider Internal Networks. Determine if the Cloud Service Provider has appropriate configurations or technical measures in place to segment the Cloud Service Delivery Networks and Cloud Service Provider Internal Networks, and to disallow any direct access to these networks. In addition, determine that the Cloud Service Provider only allows direct access via controlled access point with 2-factor authentication.	√	√	
24.3 Network protection					
24.3.3(c) Incremental	24.3.3(a)	CSA CCM does not require the prohibition of direct public access to systems hosting sensitive data. Determine if the Cloud Service Provider is prohibiting direct public access to systems hosting sensitive data.		√	
24.3.3(d) Incremental	24.3.3(a)	CSA CCM does not cover stateful inspection. Determine if the Cloud Service Provider has put in place controls and configurations for stateful inspection.		√	
24.3.3(e) Incremental	24.3.3(a)	CSA CCM does not include prevention of internal IP address disclosure. Determine if the Cloud Service Provider has put in place configurations to prevent the disclosure of internal IP addresses.		√	
24.5 Storage area networks (SANs)					
24.5.3(c) Incremental	24.5.3(a)	CSA CCM does not cover mutual authentication between devices. Determine if the Cloud Service Provider is leveraging mutual authentication between devices on the storage area networks (SANs).	√	√	

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
24.5.3(d) New	24.5.3(a)	Determine if the Cloud Service Provider has implemented configurations or technical measures to ensure that storage devices in storage area networks (SANs) will and / or can only respond to requests from authorised devices.	√	√	
24.5.3(e) New	24.5.3(a)	Determine if the Cloud Service Provider has implemented configurations or technical measures to ensure that automatic replication of data stored in the storage area networks (SANs) is disallowed.	√	√	
24.6 Data segregation					
24.6.3(a)-(b) Incremental	24.6.3(a)	CSA CCM does not cover logical segregation for data access, logs, and encryption keys, and offsite data storage. Determine if the Cloud Service Provider has implemented configurations such that logical segregation of data access, logs, and encryption keys is kept at a minimum. Also, determine if the same segregation controls has been applied to offsite data storage and recovery.	√	√	

8.3 MTCS SS Level 3

This section summarises the audit guidance for gaps identified between MTCS SS Level 3 and CSA STAR. Identified gaps between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 are highlighted in the Gap Analysis Report and these clauses are not included in this report.

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6 Information security management					
6.5 Review of information security policy					
6.5.3(a) Incremental	6.5.4(a)	CSA CCM does not specifically require the review of the information security policy to be conducted at least twice annually. Determine if the Cloud Service Provider has effectively conducted reviews for the Information Security Policy, at least twice in a year.	√		√
6.6 Information security audits					
6.6.2(a)-(b) Incremental	6.6.4(a)	CSA CCM does not cover the establishment of an audit committee and the approval of IT security audit plans by a formal 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). In addition, determine if the following controls have been implemented: • IT security audit plans have been approved by the audit committee formed as per MTCS SS Requirement 6.6.2(a). • audit scope addresses the right level of testing based on the organisation's risk assessment. • audit scope covers the review of the risks faced by the organisation and identification of any potential control weaknesses.	√		√
7 Human resources					
7.1 Background screening					
7.1.4(a) Incremental	7.1.4(a)-(b)	CSA CCM does not explicitly state the frequency of background checks. Determine if the Cloud Service Provider has conducted annual background checks for all personnel and they have been reviewed by the management. Refer to MTCS SS Requirement 7.1.4(a) for examples of persons falling under this category.	√		
7.2 Continuous personnel evaluation					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
7.2.4(a) New	7.2.4(a)-(b)	CSA CCM does not require the annual evaluation of personnel security. Determine if the Cloud Service Provider has put into place policy and procedural measures to have the evaluation of personnel security to be conducted at least on an annual basis.	√		
7.3 Employment and contract terms and conditions					
7.3.4(a) Incremental	7.3.4(a)	While acknowledgement can be implied from the signing of employment contract as covered in CSA CCM, the need for re-acknowledgement is not included. Determine if the Cloud Service Provider require employees and relevant third parties to re-acknowledge the acceptance of Information Security Obligations Agreement at least on an annual basis and prior to the termination of service.	√		
8 Risk management					
8.1 Risk management program					
8.1.4(a) Incremental	8.1.4(a)-(b)	CSA CCM does not require risk metrics. Determine if the Cloud Service Provider has evaluated risk metrics, in addition to risks and mitigation steps. In addition, determine if the Cloud Service Provider has established plans for addressing residual risks at least on a quarterly basis. Furthermore, through interviews, verify the frequency of risk assessment and validate that the outcome of risk assessment has been incorporated into the organisation's security strategy.	√		√
8.4 Risk register					
8.4.3(a) Incremental	8.4.4(a)	CSA CCM does not specifically require the establishment of a risk register containing the risk attributes stated in MTCS SS Requirement 8.4.3(a) for risk management. Determine if the Cloud Service Provider has established a risk register defining the abovementioned risk attributes in the risk management process and there is a corresponding mitigation plan for each type of identified risk.	√		
9 Third party					
9.4 Third party delivery management					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
9.4.4(d) Incremental	9.4.4(d)	While CSA CCM covers periodic reviews on third parties, the specific need for onsite visits is not explicitly mentioned. Determine if the Cloud Service Provider has conducted onsite visits to the third party service provider's data centres to assess the quality of its data centre's operation and security controls.	√		√
10 Legal and compliance					
10.3 Prevention of misuse of cloud facilities					
10.3.2(b), (d)-(e) Incremental	10.3.4(a)	CSA CCM does not cover in detail requirements for prevention of misuse of cloud facilities. Determine if the following controls have been implemented: • training sessions pertaining to the monitoring policies, procedures and tools in place have been conducted; • monitoring for detecting if the cloud infrastructure is being used as a platform to attack others; • inclusion of access and monitoring policies / restrictions in third party contracts and agreements; and • effective implementation of controls to prohibit misuse of cloud facilities.	√	√	√
10.6 Continuous compliance monitoring					
10.6.4(a) New	10.6.4(a)	CSA CCM does not cover the provision of real-time monitoring for cloud users. Determine if the Cloud Service Provider has a mechanism in place to allow cloud users to monitor security of the cloud environment specific to the type of cloud services provided to these users.	√	√	√
11 Incident management					
11.2 Information security incident response plan testing and updates					
11.2.4(a) New	11.2.4(a)-(b)	CSA CCM does not require incident drills to be conducted. Determine if the Cloud Service Provider has conducted incident drills at least twice a year with defined escalation response time and in-depth involvement and reporting from interested parties. In addition, verify if the plan has been updated with the lessons learnt from the previous drill.	√		√
12 Data governance					
12.5 Data protection					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
12.5.4(a) Incremental	12.5.4(a)	While CSA CCM covers data loss and prevention in general, it does not explicitly require a data loss prevention strategy. Determine if the Cloud Service Provider has implemented a data loss prevention strategy that should address the data at the areas as stated in MTCS SS clause 12.5.4(a).	√	√	√
12.7 Data backups					
12.7.2(a) Incremental	12.7.4(a)	CSA CCM does specify controls for encryption of backups stored off-site. Determine if appropriate cryptographic controls are in place to protect backups before they are transported to be stored off-site. In addition, perform a sample check to validate if backups can be restored.			√
12.8 Secure disposal and decommissioning of hardcopy, media and equipment					
12.8.2(c) Incremental	12.8.4(a)	CSA CCM does not specifically cover the secure disposal and decommissioning procedures of hardcopy materials. Determine if the Cloud Service Provider has established secure disposal procedures for hardcopy, media and equipment, which include methods as stated in MTCS SS Requirement 12.8.2(c), by physically inspecting the shredding facility to assess the sufficiency of the security. Alternatively, verify if the cloud service provider has obtained a "Certificate of Destruction" from a data disposal third party as evidence of secure disposal.			√
13 Audit logging and monitoring					
13.2 Log review					
13.2.4(a) New	13.2.4(a)-(b)	CSA CCM does not require a tool to monitor logs in real time. Determine if the Cloud Service Provider has implemented an automated tool for real time monitoring of logs and that the logs have been configured appropriately and are capturing the necessary information.	√	√	√
14 Secure configuration					
14.1 Server and network device configuration standards					
14.1.4(a) New	14.1.4(a)	CSA CCM does not cover the Common Criteria EAL4 certification. Determine if the Cloud Service Provider is only deploying systems and infrastructure that have been Common Criteria EAL4 or similarly certified.	√		√
14.2 Malicious code prevention					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
14.2.4(a) Incremental	14.2.4(a)	While CSA CCM requires the use of anti-malware programs, it does not specifically require the testing of prevention and detection capabilities of these anti-malware programs. Determine if the Cloud Service Provider has conducted periodic testing of the prevention and detection capabilities and recovery procedures of the anti-malware programs used in the cloud infrastructure against malicious code.	√		√
14.2.4(b) Incremental	14.2.4(b)	CSA CCM does not specifically require that user-provided code is sandboxed or isolated. Determine if the Cloud Service Provider has policies and procedural measures in place to ensure that any user-provided code is sandboxed or isolated.	√	√	√
14.9 Enforcement checks					
14.9.4(a) Incremental	14.9.4(a)-(b)	CSA CCM requires checks on security configurations to be performed on an annual basis instead of on a daily basis. Determine by reviewing the enforcement report if the Cloud Service Provider has conducted daily checks on security configurations against baseline standards.	√		√
14.9.4(b) Incremental	14.9.4(c)	While CSA CCM requires the implementation of file integrity monitoring tools, the specific requirement to raise alerts immediately when required is not mentioned. Determine if the Cloud Service Provider has implemented file integrity monitoring tools to alert immediately of any unauthorised modification of critical systems, configurations and content files.	√	√	√
15 Security testing and monitoring					
15.1 Vulnerability scanning					
15.1.4(a) Incremental	15.1.4(a)-(b)	CSA CCM requires vulnerability scanning to be conducted on an annual basis instead of on a monthly basis. Determine if the Cloud Service Provider has conducted vulnerability scannings at least on a monthly basis. In addition, validate if the scans, assessment and corresponding mitigation plans are effective.	√		√
15.2 Penetration testing					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
15.2.4(a) Incremental	15.2.4(a)-(b)	CSA CCM does not specify a frequency for conducting penetration tests. Determine if the Cloud Service Provider has conducted internal and external penetration tests at least twice annually and verify the effectiveness of the penetration testing program, including follow-up of identified findings.	√		√
15.3 Security monitoring					
15.3.4(a) Incremental	15.3.4(a)-(c)	While elements of security monitoring are present in CSA CCM, details pertaining to the depth and scope of the reviews are not included. Determine if the Cloud Service Provider has included the following requirements in its security monitoring process: • frequency of technical compliance reviews; • sufficiency of technical depth and scope of review; and • due diligence in selecting personnel performing the reviews.	√		√
16 System acquisitions and development					
16.2 Web application security					
16.2.4(a) Incremental	16.2.4(a)	CSA CCM does not cover the testing of web services. Determine if the Cloud Service Provider has tested web application security of private / protected interfaces.	√		√
17 Encryption					
17.3 Key management					
17.3.4(a) Incremental	17.3.4(a)	While CSA CCM requires policies and procedures to be established for the management of cryptographic keys, details relating to storage of cryptographic keys are not mentioned. Determine if the Cloud Service Provider is storing cryptographic keys in tamper-resistant devices.	√	√	√
18 Physical and environmental					
18.3 Physical access					
18.3.3(a) Incremental	18.3.4(a)	Determine if the Cloud Service Provider has implemented effective physical security and access logging controls, including, monitoring individual access to areas hosting sensitive data and storing access logs for at least three (3) months.		√	√
19 Operations					
19.5 Reliability and resiliency					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
19.5.4(h) Incremental	19.5.4(a)-(b)	CSA CCM does not cover details relating to the reliability and resiliency of storage systems. Determine if the Cloud Service Provider has fulfilled specific requirements listed in MTCS SS Requirements 19.5.4(b)-(c) and 19.5.4(e)-(h) to enhance storage, network security management, backup and information security components.	√	√	√
20 Change management					
20.3 Back-out or rollback procedures					
20.3.4(a) Incremental	20.3.4(a)	While CSA CCM covers change management in general, it does not cover alternate recovery options. Determine if the Cloud Service Provider has explored alternate recovery options if the change applied is not successfully implemented in the production environment and cannot be rolled back to a former version.	√		√
20.5 Patch management procedures					
20.5.4(a) Incremental	20.5.4(a)	While CSA CCM specifies that patches should be implemented, it does not require that patches not applied within a specific time frame be justified and tracked to closure. Determine if the Cloud Service Provider has policies and procedural measures in place to justify why patches are not implemented, and tracking to closure.	√		√
21 Business continuity planning (BCP) and disaster recovery (DR)					
21.1 BCP framework					
21.1.3(b) Incremental	21.1.4(a)	Determine if the Cloud Service Provider has established Recovery Point Objective (RPO) for each of their service offering including sufficiency of geographical distribution of failover locations.	√		√
21.2 BCP and DR plans					
21.2.4(a) Incremental	21.2.4(a)	While CSA CCM covers backup requirements in general, it does not require the implementation of backup capabilities at the individual system or application cluster level. Determine if the Cloud Service Provider has implemented rapid operational and backup capabilities at the individual system or application cluster level.	√	√	√
21.2.4(c) Incremental	21.2.4(b)	CSA CCM covers Recovery Time Objective (RTO) but does not cover Recovery Point Objective (RPO). Determine if the Cloud Service Provider has considered interdependencies between critical information assets and has defined recovery and business resumption priorities for targets.	√		√

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
21.3 BCP and DR testing					
21.3.4(a) Incremental	21.3.4(a)-(b)	CSA CCM does not define a specific frequency for the testing of business continuity plans. Determine if the Cloud Service Provider has tested business continuity and disaster recovery plans, updated those plans at least on an annual basis, and included plans for various test case scenarios (refer to MTCS SS clause 21.3.4(a) for examples). In addition, verify the appropriate test cases for BCP, and validate if the BCP and DR plan have been updated annually and signed off by the management.	√		√
22 Cloud services administration					
22.6 Password reset and first logon					
22.6.4(a) Incremental	22.6.4(a)	CSA CCM does not specifically require that half of the new password be sent to the owner and the other half be sent to their supervisor. Determine if the Cloud Service Providers have implemented appropriate mechanism such that half of the new password is provided via an out-of-band mechanism directly to the affected person and the other half is provided to their supervisor.	√	√	√
22.7 Administrator access security					
22.7.4(a) Incremental	22.7.4(a)	CSA CCM does not specifically require the use of privilege access management tools. Determine if the Cloud Service Provider has implemented privilege access management tools to restrict administrators' direct access to privileged functions and accounts.	√	√	√
22.9 Session management					
22.9.2(a) Incremental	22.9.4(a)	CSA CCM does not specifically cover details about reactivation of idle sessions. Determine the effectiveness of the session management controls implemented by the Cloud Service Provider.	√	√	√
22.10 Segregation of duties					
22.10.4(a) Incremental	22.10.4(a)-(b)	CSA CCM does not specify a frequency for the reviews of access rights and segregation of duties. Determine if the Cloud Service Provider has conducted reviews for access rights and segregation of duties at least on a monthly basis and assess the effectiveness of segregation of duty controls in mitigating risks faced by the organisation.	√		
22.12 Third party administrative access					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
22.12.4(a) Incremental	22.12.4(a)	CSA CCM does not explicitly require that third party access to the environment be allowed only under the supervision of the Cloud Service Provider's personnel. Determine if the Cloud Service Provider allows third party access to the environment 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)	CSA CCM does not cover the change of passwords for service accounts. Determine if the Cloud Service Provider has established procedures to change service account passwords at least twice annually or when an administrator leaves the organisation. Validate the above through identifying the timeframe between the administrator's last day in office and password change implementation date.	√		
23 Cloud user access					
23.2 User access security					
23.2.4(a) New	23.2.4(a)	CSA CCM does not specifically require the restriction of storage of the same user identity in multiple environments. Verify that the Cloud Service Provider is not storing the same user identities in multiple cloud environments.	√	√	√
23.6 Password protection					
23.6.2(a)-(c) Incremental	23.6.4(a)	While CSA CCM covers access control requirements in general, specific controls as stated in MTCS SS clause 23.6.2 are not included. Determine if the Cloud Service Provider has following controls covered in the approved hardening documents: • all passwords are rendered unreadable during transmission; • passwords are transmitted through encrypted channels; and • password storage is encrypted to protect passwords. In addition, verify if system configuration reviews have been conducted to validate that information systems are configured in accordance with approved hardening documents.		√	√
23.7 User session management					

MTCS Clause / Requirement	MTCS SS Audit Procedure	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
23.7.4(a) Incremental	23.7.4(a)-(c)	While CSA CCM covers access control in general, it does not specifically require connection time for applications to be restricted. Determine if the Cloud Service Provider has effective controls in place for implementing maximum connection time of applications, as part of approved hardening documents. In addition, verify if system configuration reviews have been conducted to validate that information systems are configured in accordance with approved hardening documents.		√	√
24 Tenancy and customer isolation					
24.1 Multi tenancy					
24.1.4(a) Incremental	24.1.4(a)	While CSA CCM covers intrusion detection in general, the specific requirement for such monitoring mechanisms is not mentioned. Determine if the Cloud Service Provider has implemented monitoring mechanisms to detect when a virtual host attempts to access another virtual host.	√	√	√
24.5 Storage area networks (SANs)					
24.5.4(a)-(b) New	24.5.4(a)	CSA CCM does not cover hard zones and Logical Unit Numbers (LUN). Determine if the Cloud Service Provider has implemented SANs configuration as per the details specified in MTCS SS clause 24.5.4.	√	√	√
24.6 Data segregation					
24.6.4(b) Incremental	24.6.4(b)	While CSA CCM requires controls to segment user access, it does not explicitly require the segregation of backups. Determine if the Cloud Service Provider has policies, procedural or technical measures in place to ensure that backups are segregated by users.	√	√	√

<End of Audit Checklist Report>