INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

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

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

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

The experts of the Working Group are affiliated with:

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

The Multi-tiered Cloud Security cross-certification Focus Group on 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 Implementation Guideline Report is the second report in the set of three (3) documents to assist Cloud Service Providers that are CSA STAR certified based on CCM v3.0 and ISO/IEC 27001:2013 to adopt MTCS SS. The purpose of each document is described in the diagram below.

Gap Analysis Report	Implementation Guideline Report	Audit Checklist Report
The purpose of the Gap Analysis Report is to provide an overview of the differences between the requirements listed in MTCS SS and 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 Implementation Guideline 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 audit function, MTCS SS certification bodies and external audit bodies on the differences between MTCS SS and CSA STAR, and the corresponding implementation guideline.

4 Document Structure

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

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

5 Terms and Definitions

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

6 Scope

In order to assist entities that are CSA STAR certified to adopt the MTCS SS, we have developed this Implementation Guideline Report for the gaps identified in Gap Analysis Report, which are classified as “INCREMENTAL” or “NEW”.

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

Gap Classification	Description
INCREMENTAL	Indicates the clauses in MTCS SS that are stated with more details than the corresponding sections in clauses in 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 the 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 clauses 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.

7 Tips on Using this Implementation Guideline Report

This document is meant to help Cloud Service Providers who are CSA STAR certified and are implementing or planning to implement the MTCS SS Levels 1, 2 or 3. The guidelines are generic and Cloud Service Providers will need to tailor the suggested guidelines to their specific requirements.

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

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

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

Similarly, reviews and / or audits are mentioned in MTCS SS Clauses 6.5 ‘Review of information security policy’, 6.6 ‘Information security audits’, 13.0 ‘Audit logging and monitoring’ and 18.6

'Physical security review'. The Cloud Service Providers can choose to structure their reviews and / or audits in a single exercise or across multiple reviews and / or audits as per organisation's preference.

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

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

8 Implementation Guidelines

8.1 MTCS SS Level 1

This section summarises the implementation guidelines for gaps identified between MTCS SS Level 1 and 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	Implementation guidance	Additional context on gaps identified on CSA CCM
6 Information security management		
6.1 Information security management system (ISMS)		
6.1.2(e) Incremental	CSA CCM does not cover risk mitigation specific to authorised insiders. The Cloud Service Provider shall implement controls to mitigate risks from authorised insiders (including internal and third parties) by considering the following measures: • Scope of risk mitigation relevant to authorised insiders to cover security policies and procedures, security infrastructure design and implementation, approval structure for operations, user access matrix, audit trail and usage logs, and tenancy and customer isolation procedures (including virtualisation). • Consider implementing an identity management system to coordinate authentication and authorisation, including some form of password management control such as different user access profiles for different areas of the system, and clear access approval structure for specific areas. Refer to MTCS SS Clause 22 for additional details.	CSA CCM covers risk management process; however, it does not explicitly define risk relating to insiders.
6.1.2(j) Incremental	CSA CCM does not cover security controls specific to virtualisation. The Cloud Service Provider shall implement controls related to virtualisation security for cloud services in policies and procedures including, but not limited to the list of areas mentioned in MTCS SS Clause 6.1.2(j). See TR 30:2012 Technical Reference for Virtualisation Security for servers for additional details.	CSA CCM does not require virtualisation specific controls in ISMS.
6.5 Review of information security policy		
6.5.2(a) Incremental	CSA CCM does not specifically require annual review of the information security policy. The Cloud Service Provider shall review its information security policy, at a minimum, on an annual basis.	While CSA CCM requires that the information security policy be reviewed at planned intervals, it does not specifically require the frequency of review to be at least annually.
6.6 Information security audits		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
6.6.2(a) Incremental	CSA CCM does not cover the establishment of an audit committee and the associated committee responsibilities. The Cloud Service Provider shall establish a formal / informal audit committee that contains, at a minimum, the members as stated in MTCS SS Clause 6.2.2(a).In addition, IT security audit plans shall be approved by the above mentioned audit committee.	While CSA CCM covers audit planning and audit activities in general, the specific requirement of an audit committee is not mentioned.
6.6.2(b) Incremental		While CSA CCM covers the approval of audit plans by stakeholders, it does not specifically require the approval from an audit committee.
8 Risk management		
8.2 Risk assessment		
8.2.2(b) Incremental	CSA CCM does not specifically require risk assessments to include risks relating to the elements as stated in MTCS SS. The Cloud Service Provider shall include, at a minimum, the types of risks listed in MTCS SS Clause 8.2.2(b) in its risk assessments.	While CSA CCM covers risk assessment in general, it does not specifically require these assessments to include risks relating to those as stated in MTCS SS.
10 Legal and compliance		
10.3 Prevention of misuse of cloud facilities		
10.3.2(b) Incremental	CSA CCM does not specifically require the inclusion of the monitoring controls in awareness and training programs. The Cloud Service Provider shall include in its awareness and training programs the monitoring controls in place to detect unauthorised access as listed in MTCS SS Clause 10.3.2(b).	While CSA CCM mentions about putting controls in place for providing appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization, it does not explicitly mandate controls to create awareness of the monitoring in place.
10.3.2(d) Incremental	CSA CCM does not specifically require monitoring controls to be in place to detect if the cloud infrastructure is being used as a platform to attack others. The Cloud Service Provider shall implement appropriate procedural and technical measures to detect usage of the cloud infrastructure as a platform to attack others.	While CSA CCM defines monitoring controls in general, it does not specify implementation of monitoring controls to detect if the infrastructure is being used for attack.
10.6 Continuous compliance monitoring		
10.6.2(a) Incremental	CSA CCM does not cover the provision of continuous or real-time compliance monitoring. Cloud Service Providers shall implement a system configuration compliance reporting framework for the purposes as stated in MTCS SS Clause 10.6.2(a).	While CSA CCM specifies controls to ensure that network environments and virtual instances shall be designed and configured to restrict and monitor traffic, it does not explicitly cover the areas mentioned in MTCS SS Clause 10.6.2 (a) on monitoring. A separate standard, CSA STAR Continuous Monitoring is under development; however, our current review is for CSA STAR Certification.
11 Incident management		
11.2 Information security incident response plan testing and updates		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
11.2.2(b) Incremental	The Cloud Service Provider shall include the following components in the incident response plan testing: • types of tests; • test scope; and • parties to be involved in the test execution and review. In addition, appropriate training shall be conducted for personnel assigned with information security incident response responsibilities.	While CSA CCM mentions general controls related to incident management including testing at planned intervals, it does not specify testing to be conducted annually.
12 Data governance		
12.5 Data protection		
12.5.2(a) Incremental	CSA CCM does not cover specific controls for media handling for virtualised images and snapshots. Cloud Service Providers shall establish controls and procedures to protect data from loss and destruction and implement security controls over access to all media (as stated in MTCS SS Clause 12.5.2(a)), including virtualised images and snapshots.	While CSA CCM defines that controls should be implemented for data protection and access control, it does not explicitly cover access to all media, virtualised images and snapshots.
12.7 Data backups		
12.7.2(a) Incremental	CSA CCM does not specify controls for encryption of back-ups stored off-site. Cloud Service Providers shall protect, with appropriate levels of encryptions and other means, back-ups before that are transported to be stored off-site.	While CSA CCM defines policies and procedures on data inventory and process flows, it does not specify controls for encryption of back-ups stored off-site.
12.7.2(c) Incremental	CSA CCM does not specifically require the knowledge of access and storage locations of back-ups. Cloud Service Providers shall maintain a list of and documentation of the access and storage locations of backups.	While CSA CCM specifies backup procedure, it does not mention access and storage location of backups.
12.8 Secure disposal and decommissioning of hardcopy, media and equipment		
12.8.2(c) Incremental	CSA CCM does not specifically cover the secure disposal and decommissioning procedures of hardcopy materials. Cloud Service Providers shall establish secure disposal procedures for the hardcopy, media and equipment, which include methods as stated in MTCS SS Clause 12.8.2(c), so that data cannot be reconstructed. Alternatively, it may obtain a "Certificate of Destruction" from a data disposal third party as evidence of secure disposal.	While risks related to data disposal, and disposal for soft copy materials are mentioned, CSA CCM does not specify controls for disposal of hardcopy materials.
14 Secure configuration		
14.1 Server and network device configuration standards		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
14.1.2(b) Incremental	CSA CCM does not cover detailed components of the controls for network security management. Refer to MTCS SS Clause 14.1.2(b)-(e) for specific requirements regarding server and network device configuration standards.	While CSA CCM has defined configuration controls, it does not require that vendor-supplied default configuration settings be changed before installing a system on the network.
14.1.2(d) Incremental		While CSA CCM requires protection of hypervisors in general, it does not specifically require hypervisor log analysis, integrity checks, or self-integrity checks to be conducted periodically.
14.1.2(e) Incremental		While CSA CCM has defined configuration controls, it does not explicitly require clipboard or file-sharing services to be disabled.
14.2 Malicious code prevention		
14.2.2(e) Incremental	CSA CCM does not cover specific control requirements for malicious code. Refer to MTCS SS Clause 14.2.2(c)-(f) for specific control requirements to address malicious code prevention.	While CSA CCM requires the use of anti-malware programs, it does not specifically require the updating of signatures at least on a daily basis or when the vendor releases a new update.
15 Security testing and monitoring		
15.1 Vulnerability scanning		
15.1.2(a) Incremental	Cloud Service Providers shall conduct vulnerability scanning at least on quarterly basis. They must address vulnerabilities with a Common Vulnerability Scoring System (CVSS) base score of 7-10 within one week. CVSS is an industry open standard designed to convey vulnerability severity and helps determine urgency and priority of response. Cloud Service Providers are recommended to adopt the CVSS standard for rating vulnerabilities.	CSA CCM requires that vulnerability scanning be performed at least on an annual basis instead of a quarterly basis.
15.1.2(b) Incremental		While CSA CCM requires that vulnerabilities be remediated, it does not cover the use of the CVSS scoring and that vulnerabilities with a score of 7-10 are addressed within a week.
15.2 Penetration testing		
15.2.2(a) Incremental	Network layer and application layer penetration testing from locations as specified in MTCS SS Clause 15.2.1 shall be conducted by the Cloud Service Provider at least on an annual basis, and logs and reports of penetration tests conducted and relevant follow-up actions shall be maintained.	CSA CCM does not specify a frequency for conducting penetration tests.
16 System acquisitions and development		
16.1 Development, acquisition and release management		
16.1.2(b) Incremental	While CSA CCM requires applications to be developed as per industry standards, it does not include additional details relevant to the development and acquisition of components as stated in MTCS SS Clause 16.1.2. Cloud Service Providers shall remove components as stated in MTCS SS Clauses 16.1.2(b) and 16.1.2(c) before production systems become active. In addition, Cloud Service Providers are to use static code	While CSA CCM requires applications to be developed as per industry standards, it does not explicitly require the removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.
16.1.2(j) Incremental		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
	analysis tools against all source code and ensure that all source codes have been established as being authentic.	While CSA CCM requires ongoing source code review, it does not specifically require the use of static code analysis tools against all source code.
16.1.2(k) Incremental		While CSA CCM requires ongoing source code review, it does not specifically require verification methods (e.g., checksum) to establish its authenticity.
17 Encryption		
17.3 Key management		
17.3.2(d) Incremental	CSA CCM does not specifically require the formal acknowledgement of responsibilities from cryptographic key custodians. Cloud Service Providers shall require cryptographic key custodians to formally and explicitly acknowledge their responsibilities as key custodians.	CSA CCM specifies controls to designate key custodians; however, it does not specify controls for obtaining formal acknowledgement of responsibilities from them.
17.4 Electronic messaging security		
17.4.2(c) Incremental	CSA CCM does not explicitly define controls for electronic messaging. Refer to MTCS SS Clause 17.4.2(a)-(f) for specific control requirements to address electronic messaging security.	While CSA CCM mentions general information security controls, it does not define specific controls for electronic messaging.
17.4.2(d) Incremental		
17.4.2(e) Incremental		
17.4.2(f) Incremental		
18 Physical and environmental		
18.4 Visitors		
18.4.2(a) Incremental	CSA CCM does not specify security controls to address security related to visitors. Cloud Service Providers shall: • ensure authorised visitors are escorted by staff; • differentiate visitors and on-site personnel using identification pass or badge; • maintain a visitor log; and • review the above-mentioned visitor log periodically.	CSA CCM does not define specific security controls to control and restrict visitor access via the use of escorts.
18.4.2(b) Incremental		CSA CCM does not define specific security controls to control and restrict visitor access through the usage of different badges.
18.4.2(c) Incremental		CSA CCM does not define specific security controls to control and restrict visitor access via logs.
18.4.2(d) Incremental		CSA CCM does not define specific security controls to control and restrict visitor access via logs that are periodically reviewed.
18.6 Physical security review		
18.6.2(b) Incremental	CSA CCM does not specifically require the periodic review of the organisation's physical security. Cloud Service Providers shall conduct reviews for its physical security at least on an annual basis.	CSA CCM defines that reviews need to be performed annually; however, it does not define specific controls to perform periodical review of physical security.
20 Change management		
20.5 Patch management procedures		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
20.5.2(b) Incremental	CSA CCM does not cover patch management procedures for dormant / offline systems. A patch management procedure shall be put in place for systems that have been dormant / offline for a period of time by the Cloud Service Provider and kept updated and relevant.	While CSA CCM does mention that patches should be applied and operating system should be hardened, it does not explicitly state that it should be that dormant or offline systems should be configured to meet hardening standards.
22 Cloud services administration		
22.2 Generation of administrator passwords		
22.2.2(c) Incremental	CSA CCM does not cover specific criteria for administrator passwords. Cloud Service Providers shall ensure that minimum password criteria follow industry standard practices as stated in MTCS SS Clause 22.2.2(a). In addition, Cloud Service Providers shall disallow generic passwords via system and application configuration as well as prepare documentation on minimum password criteria, and shared passwords with other accounts.	While CSA CCM requires password policies to be documented and enforced, it does not specifically require that shared passwords with other accounts be disallowed.
22.3 Administrator access review and revocation		
22.3.2(c) Incremental	While CSA CCM covers the account management controls in general, the specific frequency to perform such review is not included. A formal access review and revocation process shall be established by the Cloud Service Provider to review the adequacy of privileges and access levels, and de-provision or remove access in a timely manner, which includes removal or disabling of inactive accounts at least every ninety (90) days and notify the relevant parties of the action taken above.	While CSA CCM defines account management controls, it does not require removal of inactive accounts every 90 days.
22.4 Account lockout		
22.4.2(a) Incremental	While CSA CCM covers user access controls in general, specific requirements as stated in MTCS SS Clause 22.4.2 are not mentioned. A formal process to detect and terminate unauthorised access attempts in a timely manner shall be implemented by the Cloud Service Provider. Account lockout requirements shall also be established based on the risk assessments and sensitivity of the system and data. Minimally, the requirements defined in MTCS SS Clause 22.4.2 shall be implemented.	While CSA CCM defines user access controls, it does not specifically allow a maximum of six (6) unsuccessful attempts.
22.4.2(b) Incremental		While CSA CCM defines user access controls, it does not specify lockout duration.
22.5 Password change		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
22.5.2(b) Incremental	While CSA CCM covers some elements of password change, details as stated in MTCS SS Clause 22.5.2 are not included. The Cloud Service Provider shall enforce compulsory password change based on industry standard practices. The new passwords should also satisfy the requirement as stated in MTCS SS Clause 22.5.2(b).	While CSA CCM requires password policies to be documented and enforced, it does not specifically require that the new passwords shall be different from the previous three (3) passwords.
22.6 Password reset and first logon		
22.6.2(a) Incremental	CSA CCM does not cover details on password reset and change, and two-factor authentication (2FA). The Cloud Service Provider shall ensure: • unique passwords are generated and users are required to change their passwords upon first login; • verification of identity before password change is continued or processed; • management approval is obtained when a password reset is requested; and • in the event that the 2FA device is lost, the password shall be reset.	CSA CCM does not specifically require the generation of unique passwords and mandating of password change upon first login.
22.6.2(b) Incremental		CSA CCM does not specifically require the verification of identity prior to changing password.
22.6.2(c) Incremental		CSA CCM does not specifically require management approval to be obtained in the event of a password reset.
22.6.2(d) Incremental		CSA CCM does not specifically require the reset of password in the event of the second factor device being lost.
22.7 Administrator access security		
22.7.2(a) Incremental	CSA CCM does not explicitly require access to be restricted to the Cloud Service Management Network and Cloud Service Delivery Network. Cloud Service Providers shall have configurations 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.	While CSA CCM states that traffic should be restricted, it does not explicitly require access to be allowed only from the Cloud Service Provider Internal Network and from specific IP addresses.
22.7.2(e) Incremental	Cloud Service Providers shall have policies and configurations in place to restrict the use and access of local administrative accounts. Explicit approval shall also be obtained if local administrative access is enabled or required. Also, administrative access shall be controlled via role-based access control mechanisms.	While policies and procedures on user access are mentioned, CSA CCM does not require that administrative access be controlled through role-based access control mechanisms.
22.9 Session management		
22.9.2(b) Incremental	CSA CCM does not specifically cover details about reactivation of idle sessions. Cloud Service Providers shall have configurations in place to require the re-entering of passwords to reactivate terminals after session idle time of more than 15 minutes.	While CSA CCM covers session lockout in general, it does not specifically require that passwords be re-entered to reactivate terminal after session idle time of more than 15 minutes.
22.10 Segregation of duties		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
22.10.2(a) Incremental	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. The Cloud Service Provider shall ensure that the review of access rights and segregation of duties is done at least on an annual basis. Individuals shall also be restricted from accessing backup and production systems.	While CSA CCM covers access rights review and segregation of duties, it does not specifically such review to be conducted annually.
22.13 Service and application accounts		
22.13.2(a) Incremental	CSA CCM does not cover details on service and application accounts, the Cloud Service Provider shall ensure that all service and application accounts are created in accordance with the requirements as stated in MTCS SS Clause 22.13.2(a).	While CSA CCM defines controls for user access policies and procedures, it does not explicitly cover service and application accounts.
23 Cloud user access		
23.2 User access security		
23.2.2(c) Incremental	CSA CCM does not cover details on documented approval, having a default "deny all" setting and having anti-bot controls in place. The Cloud Service Provider shall enforce: • documented approval from authorised personnel for the granting of user access privileges; • default "deny-all" setting; • restriction of write / modify access to publicly available information; and • implementation of anti-bot controls.	While CSA CCM has defined controls for user access management, CSA CCM does not mandate to implement a default deny-all setting.
23.2.2(d) Incremental		While CSA CCM has defined controls for user access management, CSA CCM does not explicitly restrict write / modify access to publicly available information.
23.2.2(e) Incremental		While CSA CCM states that traffic should be restricted and monitored, it does not explicitly specify anti-bot controls to be implemented.
23.3 User access password		
23.3.2(c) Incremental	While CSA CCM covers password controls for mobile devices and wireless, specific password criteria as stated in MTCS SS Clause 23.3.2(a) are not mentioned. The Cloud Service Provider shall also ensure that generic passwords are not allowed and passwords cannot be shared among accounts.	While CSA CCM defines password controls for mobile devices and wireless, CSA CCM does not explicitly prohibit sharing of passwords for other devices / access methods.
23.4 User account lockout		
23.4.2(a) Incremental	CSA CCM does not cover details on account lockout. The Cloud Service Provider shall put into place configurations or measures to lock user accounts out after criteria as stated in MTCS SS Clause 23.4.2 are satisfied. Reviews shall also be conducted by the Cloud Service Provider to ensure that configurations have been put into place in accordance with hardening documents approved beforehand.	While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.4.2(b) Incremental		While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.5 User password reset and 1st logon change		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
23.5.2(b) incremental	CSA CCM does not cover details about first time logon. Cloud Service Providers shall have policies and configurations in place to require users to verify their identity before password reset is processed.	CSA CCM does not specify password controls related to first time logon.
23.6 Password protection		
23.6.2(a) Incremental	While CSA CCM covers access control requirements in general, specific controls as stated in MTCS SS Clause 23.6.2 are not included. The Cloud Service Provider shall ensure that all passwords are rendered unreadable during transmission. The channels where the transmission is performed shall also be encrypted. In addition, the Cloud Service Provider shall sufficiently protect the passwords by encrypting the password storage.	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.6.2(b) Incremental		
23.6.2(c) Incremental		
23.7 User session management		
23.7.2(a) Incremental	While CSA CCM covers access control requirements in general, specific controls as stated in MTCS SS Clause 23.7.2 are not included. The Cloud Service Provider shall have configuration 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 15 minutes; and • implement cryptographically strong identifiers for each user session.	While CSA CCM defines controls pertaining to access control, it does not define session controls.
23.7.2(b) Incremental		While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.7.2(c) Incremental		While CSA CCM defines controls pertaining to access control, it does not define session controls.
23.9 Self-service portal creation and management of user accounts		
23.9.2(a) Incremental	CSA CCM does not cover specific password criteria for self-service portals. The Cloud Service Provider shall maintain strict password criteria in accordance to requirements as defined in MTCS SS Clause 23.3.	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.10 Communication with cloud users		
23.10.2(a) Incremental	CSA CCM does not cover the availability of a secure distribution channel for official notifications. The Cloud Service Provider shall implement communication mechanisms to communicate official notifications securely to cloud users.	While CSA CCM mentions notification to cloud users, it does not specify that a procedure should be designed for distributing notifications.
24 Tenancy and customer isolation		
24.3 Network protection		
24.3.2(m) Incremental	CSA CCM does not specifically require that any traffic from the wireless network be denied to the cloud infrastructure networks and cloud service management networks. Cloud Service Providers shall configure their network firewalls to deny any traffic from the wireless environment to critical cloud infrastructure and management networks.	While CSA CCM covers wireless security in general, it does not specifically require that any traffic from the wireless network be denied to the cloud infrastructure networks and cloud service management networks.

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
24.4 Virtualisation		
24.4.2(a) Incremental	While CSA CCM covers virtualisation security in general, it does not include details as mentioned in MTCS SS Clauses 24.4.2(a) and 24.4.2(c). The Cloud Service Provider shall identify security risks including, but not limited to, those as stated in MTCS SS Clause 24.4.2(a), and address them. Also, Cloud Service Providers shall encrypt virtual machines to help protect them against theft.	While CSA CCM defines controls for infrastructure and virtualisation security, it does not explicitly cover details mentioned in MTCS SS 24.4.2(a).
24.4.2(c) Incremental		While CSA CCM requires the preservation of the integrity of virtual machines, it does not specifically require that virtual machines are to be encrypted to protect against theft.
24.5 Storage area networks (SAN)		
24.5.2(a) Incremental	CSA CCM does not cover equipment security specifically for SANs. Cloud Service Providers shall have access controls in place to limit the devices that can communicate with network attached storage devices and establish a process or procedure to ensure that changes to SANs and associated network components are correctly and accurately propagated.	While CSA CCM covers access control requirements in general, it does not specifically cover access to network attached storage devices.
24.5.2(b) Incremental		While CSA CCM defines IT governance and service management-related business processes should be implemented, it does not require the implementation of a process for propagating configuration changes and ensuring that the storage area network and associated network components are configured correctly.

8.2 MTCS SS Level 2

This section summarises the implementation guidelines for gaps identified between MTCS SS Level 2 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	Implementation guidance	Additional context on gaps identified on CSA CCM
6 Information security management		
6.5 Review of information security policy		
6.5.3(a) Incremental	CSA CCM does not specifically require the review of the information security policy to be conducted at least twice annually. The Cloud Service Provider shall conduct reviews for its information security policy at least twice annually.	While CSA CCM requires that the information security policy be reviewed at planned intervals, it does not specifically require the frequency of review to be at least twice annually.
7 Human resources		
7.1 Background screening		
7.1.3(a) Incremental	CSA CCM does not specifically require background checks for personnel with access to critical cloud infrastructure networks to be performed at specific frequencies. Cloud Service Providers shall conduct background checks for personnel with access to the Cloud Service Management Network or Cloud Service Delivery Network at least on an annual basis.	While CSA CCM states that background verification should be performed, it does not explicitly state that at least one annual background check should be performed for personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.
7.2 Continuous personnel evaluation		
7.2.3(a) New	CSA CCM does not cover frequency of continuous personnel evaluation. Cloud Service Providers shall conduct annual evaluation for personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.	CSA CCM does not require annual evaluation of personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.
7.2.3(b) New	CSA CCM does not cover the scope of coverage of personnel evaluation. Cloud Service Providers shall cover at least the items as stated in MTCS SS Clause 7.2.3(b) during personnel evaluation.	CSA CCM does not specify parameters to be covered in the annual evaluation of the personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.
8 Risk management		
8.4 Risk register		
8.4.3(a) Incremental	CSA CCM does not specifically require the establishment of a risk register containing the risk attributes stated in the MTSC SS Clause 8.4.3(a) in the risk management. Cloud Service Providers shall establish a risk register defining the abovementioned risk attributes in the risk management process.	While CSA CCM covers establishment and documentation of risk criteria, it does not specifically require the establishment of a risk register, and the inclusion of the attributes as stated in MTCS SS.
10 Legal and compliance		
10.6 Continuous compliance monitoring		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
10.6.3(a) Incremental	CSA CCM does not cover reporting requirements for system access. Cloud Service Providers shall implement a mechanism to provide system access reports to cloud users within an acceptable timeframe that was agreed upon.	While CSA CCM defines controls related to access control, it does not specify controls to provide system access reports within a defined timeframe. A separate standard, CSA STAR Continuous Monitoring is under development; however, our current review is for CSA STAR Certification.
12 Data governance		
12.6 Data retention		
12.6.3(d) Incremental	While CSA CCM requires retention controls to be in place, it does not specify the mechanisms and rules. Cloud Service Providers shall implement periodic manual or automatic processes to identify and delete all data exceeding the defined retention period.	While CSA CCM defines data retention requirements, it does not specify deletion of data beyond retention period.
13 Audit logging and monitoring		
13.2 Log review		
13.2.3(a) Incremental	Cloud Service Providers shall perform log reviews for all system components, at least on a daily basis.	CSA CCM does not explicitly require log reviews to include all critical systems and services performing security functions.
13.4 Backup and retention of audit trails		
13.4.3(b) Incremental	CSA CCM does not specify additional details with regards to logs that are accessible via the internet. Cloud Service Providers shall ensure that logs that are accessible via the internet be: • written onto a log server located on an internal network segment; and • protected by a firewall. In addition, remote access to the log server is disallowed and local access is restricted via tightly controlled user IDs.	While CSA CCM covers the lifecycle management of audit logs in general, it does not specifically require that logs that are accessible via the internet be written onto a log server located on an internal network segment protected by a firewall, and that the log server shall have no remote access and tightly controlled user IDs for local access.
14 Secure configuration		
14.9 Enforcement checks		
14.9.3(a) Incremental	Cloud Service Providers shall perform checks on its security configurations at least on a weekly basis.	CSA CCM requires checks to be performed annually instead of on a weekly basis.
15 Security testing and monitoring		
15.1 Vulnerability scanning		
15.1.3(a) Incremental	Cloud Service Providers shall conduct vulnerability scanning at least on a quarterly basis and when significant changes occur to the environment.	CSA CCM requires that vulnerability scanning be performed at least on an annual basis instead of on a quarterly basis or when significant changes occur to the environment.
15.1.3(b) Incremental	CSA CCM does not require the usage of the Common Vulnerability Scoring System (CVSS) to address vulnerabilities timely. Cloud Service Providers shall address vulnerabilities with a CVSS base score of 4-6.9 within one month.	While CSA CCM requires that vulnerabilities be remediated, it does not cover the use of the CVSS scoring and that vulnerabilities with a score of 4-6.9 are addressed within a month.
16 System acquisitions and development		
16.1 Development, acquisition and release management		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
16.1.3(a) Incremental	CSA CCM does not define controls to allow clients to verify the integrity and authenticity of the applications. Cloud Service Providers shall implement protection controls which allow the clients (e.g., web browsers and email clients) to verify the integrity and authenticity of the applications.	While CSA CCM requires implementation of strong technical controls, it does not explicitly define the implementation of controls to allow clients to verify the integrity and authenticity of the applications.
16.2 Web application security		
16.2.3(a) Incremental	CSA CCM does not specifically require the use of vulnerability security assessment tools or mechanisms. Cloud Service Providers shall review 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, these reviews should include, at the minimum, the identification of common web application vulnerabilities.	While CSA CCM covers technical security reviews (e.g., penetration testing, vulnerability assessments), it does not specifically require the use of manual or automated vulnerability security assessment tools or mechanisms annually, or when there are changes to the applications; and the inclusion of the identification of common web application flaws.
16.2.3(c) Incremental	CSA CCM does not require the security testing of public web services. Cloud Service Providers shall include public web services in security testing.	While CSA CCM defines testing controls, it does not specifically cover public servers or the inclusion of public web services in security testing.
17 Encryption		
17.3 Key management		
17.3.3(c) New	CSA CCM does not cover specific key management lifecycle process and controls. Refer to MTCS SS Clause 17.3.3 for specific requirements to be implemented by the Cloud Service Provider.	While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not mandate periodic security review of the cryptosystem.
17.3.3(d) Incremental		While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not specify controls for archival.
17.3.3(e) Incremental		While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not specify controls related to dual control on crypto-keys.
17.3.3(f) Incremental		CSA CCM states that policies and procedures shall be established for the management of cryptographic keys; however, it does not impose restriction of managing logical access independent of native operating system access control.
17.3.3(g) Incremental		While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not mention controls specific to the generation of private keys.

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
17.3.3(h) Incremental		While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not mention controls for export of private keys.
18 Physical and environmental		
18.3 Physical access		
18.3.3(a) Incremental	The Cloud Service Provider shall monitor individual access to areas hosting sensitive data and store access logs for at least three (3) months. Cloud Service Providers that adopt access card security or similar control to monitor individual access to such areas can review the access logs generated by the relevant systems.	While CSA CCM states that sensitive areas will be monitored; however, it does not explicitly state that access logs should be stored for at least 3 months.
18.4 Visitors		
18.4.3(a) New	CSA CCM does not include management approval as part of access control policy. The Cloud Service Provider shall establish management approval as a prerequisite before the visitors are allowed into facilities where sensitive data is hosted.	CSA CCM does not define specific security controls to control and restrict visitor access via obtaining management approval in specific situations.
20 Change management		
20.3 Back-out or rollback procedures		
20.3.3(a) Incremental	CSA CCM does not cover rollback plans and procedures as part of backup management. The Cloud Service Provider shall establish a procedure to rollback to a former version if problem is encountered during or after the deployment of changes.	While CSA CCM defines controls for change management process, it does not explicitly mention about designing rollback option.
20.5 Patch management procedures		
20.5.3(c) Incremental	CSA CCM does not require the testing of patches. The Cloud Service Provider shall test patches in a test environment that has a setup mirroring the production environment prior to application.	While CSA CCM defines that patches should be implemented, it does not specify controls to test the patches.
20.5.3(d) Incremental	CSA CCM does not cover hardening of dormant or offline systems. The Cloud Service Provider shall implement a process to ensure that systems that have been dormant or offline for over thirty (30) days are configured to meet hardening standards and all security software including patches are 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.	While CSA CCM does mention that patches should be applied and operating system should be hardened, it does not explicitly state that dormant or offline system should be configured to meet hardening standards and patch requirements.
21 Business continuity planning (BCP) and disaster recovery (DR)		
21.1 BCP framework		
21.1.3(b) Incremental	Cloud Service Providers shall define Recovery Point Objective (RPO) for each of their service offering.	Recovery Point Objective (RPO) is not explicitly mentioned in CSA CCM.

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
22 Cloud services administration		
22.2 Generation of administrator passwords		
22.2.3(a) Incremental	CSA CCM requires password policies to be documented and enforced but it does not include specific password criteria. The Cloud Service Provider shall implement minimum password criteria as stated in MTCS SS Clause 22.2.3(a). Alternatively, other solutions can be used where they provide equivalent or better security.	While CSA CCM requires password policies to be documented and enforced, specific details of such password policies are not mentioned.
22.4 Account lockout		
22.4.3(a) Incremental	CSA CCM does not cover details about account lockout. The Cloud Service Provider shall ensure that accounts are locked out until another administrator unlocks it manually.	While CSA CCM defines user access controls, it does not specifically require that only an administrator can manually unlock the account.
22.6 Password reset and first logon		
22.6.3(a) Incremental	CSA CCM covers password management in general but not the splitting of password. The Cloud Service Provider shall implement controls to ensure that the new password provided is split controlled and via out-of-band mechanism such that no single user has knowledge of the whole password in transit.	CSA CCM does not specifically require that new passwords be split controlled and via out-of-band mechanism, and the consideration of password management tools for higher level controls
22.7 Administrator access security		
22.7.3(a) New	CSA CCM does not cover bastion hosts. Access from the network locations as stated in MTCS SS Clause 22.7.3 shall only be permitted via bastion hosts.	CSA CCM does not require that access from the Cloud Service Provider Internal Network to the Cloud Service Management Network and Cloud Service Delivery Network is only allowed via bastion hosts.
22.10 Segregation of duties		
22.10.3(a) Incremental	Cloud Service Providers shall conduct reviews of access rights and segregation of duties at least on a quarterly basis.	While CSA CCM covers access rights review and segregation of duties, it does not specifically require such review to be conducted on a quarterly basis.
22.13 Service and application accounts		
22.13.3(a) Incremental	ISO/IEC 27001:2005 does not cover detailed requirements pertaining to service and application accounts. Refer to MTCS SS Clause 22.13.3 for specific requirements.	While CSA CCM defines controls for user access policies and procedures, it does not cover service and application accounts.
22.13.3(b) Incremental		While CSA CCM defines controls for user access policies and procedures, it does not disallow the caching or storing of sensitive session parameters, cookies or similar on local machines.
22.13.3(c) Incremental		While CSA CCM requires all the Operating System to be hardened, it does not explicitly cover restricting simultaneous logins.
22.13.3(e) Incremental		While CSA CCM requires the development of applications in accordance to industry standards, it does not specifically require the consideration of the cloud authentication model in the development of application.
23 Cloud user access		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
23.3 User access password		
23.3.3(a) Incremental	CSA CCM does not define specific criteria for passwords. The Cloud Service Provider shall implement minimum password criteria as stated in MTCS SS Clause 23.3.3(a). Alternatively, other solutions can be used where they provide equivalent or better security.	While CSA CCM defines password controls for mobile devices and wireless, CSA CCM does not define specific criteria for password settings.
23.4 User account lockout		
23.4.3(a) Incremental	CSA CCM does not cover details pertaining to account lockout. User ID shall be locked out after a maximum of six (6) unsuccessful attempts and the lockout duration to be until an administrator re-enables the user ID.	While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.4.3(b) Incremental		
23.8 Change of cloud user's administrator details notification		
23.8.3(a) Incremental	CSA CCM does not cover the alert for change in administrator details and approval being needed for changing the cloud user's administrator details. The Cloud Service Provider shall have 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 shall only be effected after the Cloud Service Provider's administrator approves the change.	While contract terms are specified to manage the supply chain, CSA CCM does not define controls to trigger alerts in specific situations.
23.8.3(b) Incremental		While contract terms are specified to manage the supply chain, CSA CCM does not specify that change in cloud User's administrator details shall need approval.
23.10 Communication with cloud users		
23.10.3(a) Incremental	CSA CCM does not specify topics for user education. The Cloud Service Provider shall provide user education on topics including, but not limited to, those as stated in MTCS SS Clause 23.10.3(a).	While CSA CCM states that information security training should be conducted, it does not explicitly define coverage of the specific topics on user access and security.
24 Tenancy and customer isolation		
24.2 Supporting infrastructure segmentation		
24.2.3(a) Incremental	While CSA CCM covers network security in general, it does not include the separation of authentication sources. The authentication sources for network locations as stated in MTCS SS Clause 24.2.3(a) shall be separated.	While CSA CCM defines controls to secure network environment, it does not cover the separation of authentication sources for Cloud Service Delivery Networks and the Cloud Service Provider Internal Networks.
24.2.3(b) Incremental	CSA CCM does not specifically require that direct access be disallowed to the Cloud Service Delivery Networks and Cloud Service Provider Internal Networks. Cloud Service Providers shall have 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. The Cloud Service Provider shall only allow direct access via controlled access point with 2-factor authentication.	While segmentation of virtualised systems is covered by CSA CCM, it does not specifically require that direct access be disallowed to the Cloud Service Delivery Networks and Cloud Service Provider Internal Networks.
24.2.3(c) Incremental		While segmentation of virtualised systems is covered by CSA CCM, it does not specifically require that direct access be disallowed to the Cloud Service Delivery Networks and Cloud Service Provider Internal Networks, or allowing direct access via controlled access point with 2-factor authentication.
24.3 Network protection		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
24.3.3(c) Incremental	CSA CCM does not require the prohibition of direct public access to systems hosting sensitive data. The Cloud Service Provider shall manage and control direct public access to systems hosting sensitive data.	While CSA CCM covers the protection of sensitive data in general with the use of appropriate levels of encryption, it does not specifically require that direct public access to systems hosting sensitive data be prohibited.
24.3.3(d) Incremental	CSA CCM does not cover stateful inspection. The Cloud Service Provider shall put in place controls and configurations to implement stateful inspection.	While CSA CCM defines controls to secure network environment, it does not explicitly cover stateful inspection.
24.3.3(e) Incremental	CSA CCM does not include prevention of internal IP address disclosure. The Cloud Service Provider shall put in place configurations to prevent the disclosure of internal IP address disclosure.	While CSA CCM defines controls to secure network environment, it does not cover the disclosure of internal IP addresses.
24.5 Storage area networks (SAN)		
24.5.3(c) Incremental	CSA CCM does not cover mutual authentication between devices. The Cloud Service Provider shall leverage mutual authentication between devices on storage area networks (SAN).	While CSA CCM defines hardening of operating system, it does not cover mutual authentication between devices.
24.5.3(d) New	Cloud Service Providers shall put in place configurations or technical measures to ensure that storage devices in storage area networks (SAN) will and/or can only respond to requests from authorised devices.	CSA CCM does not require that storage devices shall only respond to requests from authorised devices.
24.5.3(e) New	Cloud Service Providers shall put in place configurations or technical measures to ensure that automatic replication of data stored in the storage area networks (SAN) is disallowed.	CSA CCM does not cover automatic replication.
24.6 Data segregation		
24.6.3(a) Incremental	CSA CCM does not cover logical segregation for data access, logs, and encryption keys, and offsite data storage. The Cloud Service Provider shall ensure that logical segregation for data access, logs, and encryption keys is kept a minimum. The same segregation controls shall be applied to offsite data storage and recovery.	While CSA CCM covers segregation for encryption keys, segregation for data access and logs are not mentioned.
24.6.3(b) Incremental		While CSA CCM covers authorisation controls, it does not cover segregation controls for offsite data storage and recovery.

8.3 MTCS SS Level 3

This section summarises the implementation guidelines for gaps identified between MTCS SS Level 3 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	Implementation guidance	Additional context on gaps identified on CSA CCM
7 Human resources		
7.1 Background screening		
7.1.4(a) Incremental	CSA CCM does not explicitly state the frequency of background checks. Cloud Service Providers shall conduct at least one annual background check for all personnel. Refer to MTCS SS Clause 7.1.4(a) for examples of persons falling under this category.	While CSA CCM says that background verification should be performed, it does not explicitly state that it should be performed yearly.
7.2 Continuous personnel evaluation		
7.2.4(a) New	CSA CCM does not require the annual evaluation of personnel security. Cloud Service Providers shall establish policy and procedural measures on annual evaluation of personnel security.	CSA CCM does not specify controls to annually evaluate all personnel.
7.3 Employment and contract terms and conditions		
7.3.4(a) Incremental	While acknowledgement can be implied from the signing of employment contract as covered in CSA CCM, the need for re-acknowledgement is not included. The Cloud Service Provider shall require re-acknowledgement of the acceptance of Information Security Obligations Agreement from personnel at least on an annual basis and prior to the termination of service.	While CSA CCM states that security policies must be signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access, it does not require personnel to re-acknowledge acceptance of Information Security Obligations annually.
8 Risk management		
8.1 Risk management program		
8.1.4(a) Incremental	CSA CCM does not require risk metrics. Cloud Service Providers shall evaluate risk metrics and plans for addressing residual risks, at least on a quarterly basis.	While CSA CCM covers risk evaluation and treatment in general, it does not specifically require risk metrics. In addition, the specific frequency of the relevant activities required by MTCS SS is not mentioned.
9 Third party		
9.4 Third party delivery management		
9.4.4(d) Incremental	While CSA CCM covers periodic reviews on third parties, the specific need for onsite visits is not explicitly mentioned. The Cloud Service Provider shall conduct onsite visits to the third party service provider's data centres to assess the quality of its data centre operations and security controls. These data centres should, in the first place, be hosting sensitive data and / or applications.	CSA CCM requires periodic reviews to be conducted on the third party service provider; however, it does not explicitly mention that onsite visits be conducted to the third party service provider's data centres.
10 Legal and compliance		
10.6 Continuous compliance monitoring		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
10.6.4(a) New	CSA CCM does not cover the provision of real-time monitoring for cloud users. The Cloud Service Provider shall have a mechanism in place to allow cloud users to monitor to the cloud environment's security based on the type of cloud services provided to these users.	CSA CCM does not specify controls for real time monitoring. A separate standard, CSA STAR Continuous Monitoring is under development; however, our current review is for CSA STAR Certification.
11 Incident management		
11.2 Information security incident response plan testing and updates		
11.2.4(a) New	CSA CCM does not cover controls for performing incident drills. The Cloud Service Provider shall conduct incident drills at least twice a year, with defined escalation response time and in-depth involvement and reporting from interested parties.	While CSA CCM mentions general controls related to incident management, it does not specify that incident drills with specific frequency and components should be performed.
12 Data governance		
12.5 Data protection		
12.5.4(a) Incremental	While CSA CCM covers data loss and prevention in general, it does not explicitly require a data loss prevention strategy. The Cloud Service Provider shall implement a data loss prevention strategy that should address the data at the areas as stated in MTCS SS Clause 12.5.4(a).	While policies and procedures to prevent data loss and destruction are mentioned, CSA CCM does not define a specific data loss prevention strategy.
13 Audit logging and monitoring		
13.2 Log review		
13.2.4(a) New	CSA CCM does not require a tool to monitor logs on real time. The Cloud Service Provider shall implement an automated tool for real time monitoring of logs and ensure that the logs are capturing the right information necessary.	CSA CCM does not require an automated tool for real time monitoring of logs.
14 Secure configuration		
14.1 Server and network device configuration standards		
14.1.4(a) New	CSA CCM does not cover the Common Criteria EAL4 certification. Cloud Service Providers shall only deploy systems and infrastructure that have been Common Criteria EAL4 or similar certified.	CSA CCM does not require that only systems and infrastructure that have been Common Criteria EAL4 certified or similar be deployed.
14.2 Malicious code prevention		
14.2.4(a) Incremental	The Cloud Service Provider shall conduct periodic testing of the prevention and detection capabilities and recovery procedures of the anti-malware programs used in the cloud infrastructure against malicious code.	While CSA CCM requires the use of anti-malware programs, it does not specifically require that the prevention and detection capabilities and recovery procedures against malicious code are tested periodically.
14.2.4(b) Incremental	CSA CCM does not specifically require that user provided code is sandboxed or isolated. Cloud Service Providers shall have policies and procedural measures in place to ensure that any user provided code is sandboxed or isolated to prevent it from impacting other cloud users.	While CSA CCM requires that externally developed source code receives a higher level of assurance, it does not specifically require that such code be sandboxed or isolated to ensure that the underlying platform and other tenants are not affected.
14.9 Enforcement checks		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
14.9.4(a) Incremental	CSA CCM requires checks on security configurations to be performed on an annual basis instead of on a daily basis. Cloud Service Providers shall conduct checks on security configurations, at least on a daily basis.	CSA CCM requires checks to be performed annually instead of on a daily basis.
14.9.4(b) Incremental	While CSA CCM requires the implementation of file integrity monitoring tools, the specific requirement to raise alerts immediately when required is not mentioned. Cloud Service Providers shall have file integrity monitoring tools to alert immediately any unauthorised modification of critical systems, configurations and content files.	While CSA CCM requires the implementation of file integrity monitoring tools, it does not require the immediate alerting of unauthorised modification of critical systems, configurations and content files.
15 Security testing and monitoring		
15.1 Vulnerability scanning		
15.1.4(a) Incremental	CSA CCM requires vulnerability scanning to be conducted annually based on the requirement in MTCS SS Clause 15.1.4(a). Cloud Service Providers shall conduct vulnerability scanning at least on a monthly basis.	CSA CCM requires that vulnerability scanning be performed at least on an annual basis instead of on a monthly basis.
15.2 Penetration testing		
15.2.4(a) Incremental	CSA CCM does not specify a frequency for conducting penetration tests. Cloud Service Providers shall conduct penetration testing at least twice annually with at least one of the tests performed by a qualified third party.	CSA CCM does not specify a frequency for conducting penetration tests or require at least one of the tests to be executed by a qualified third party.
15.3 Security monitoring		
15.3.4(a) Incremental	The Cloud Service Provider shall include the requirements as stated in MTCS SS Clause 15.3.4(a) in its security monitoring process.	While CSA CCM requires the conducting of technical compliance reviews, it does not specify the need for scheduling it periodically, identification and establishment of technical depth and scope of review, and assessment of the technical competencies of personnel performing the reviews.
16 System acquisitions and development		
16.2 Web application security		
16.2.4(a) Incremental	CSA CCM does not cover the testing of web services. The Cloud Service Provider shall conduct web application testing and ensure that private / protected web services interfaces are included in the scope of web application tests.	While CSA CCM defines testing controls, it does not cover private / protected web services interfaces or the inclusion of private / protected web services in web application testing.
17 Encryption		
17.3 Key management		
17.3.4(a) Incremental	Cloud Service Providers shall store cryptographic keys in tamper-resistant devices.	While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not explicitly mention controls for storage of keys in tamper resistant device.
19 Operations		

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
19.5 Reliability and resiliency		
19.5.4(h) Incremental	CSA CCM does not cover details relating to the reliability and resiliency of storage systems. The Cloud Service Providers shall fulfil specific requirements listed in MTCS SS Clauses 19.5.4(b)-(c) and 19.5.4(e)-(h) to enhance storage, network security management, backup and information security components.	CSA CCM does not require the installation of capabilities for early detection of warnings and outages of storage systems.
20 Change management		
20.3 Back-out or rollback procedures		
20.3.4(a) Incremental	While CSA CCM covers change management in general, it does not cover alternate recovery options. The Cloud Service Provider shall explore alternate recovery options if a change applied is not successfully implemented in the production environment and cannot be rolled back to a former version.	While CSA CCM defines controls for change management process, it does not explicitly mention about defining alternate recovery options, in case of an unsuccessful change.
20.5 Patch management procedures		
20.5.4(a) Incremental	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. Cloud Service Providers shall have policies and procedural measures in place to justify why patches are not implemented and track such patches to closure.	While CSA CCM defines that patches should be implemented, it does not specify controls to ensure that patches that are not applied within a specific time frame, are justified and tracked to closure.
21 Business continuity planning (BCP) and disaster recovery (DR)		
21.2 BCP and DR plans		
21.2.4(a) Incremental	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. Cloud Service Providers shall implement rapid operational and backup capabilities at the individual system or application cluster level.	While CSA CCM covers backup requirements in general, it does not require the implementation of rapid operational and backup capabilities at the individual system or application cluster level.
21.2.4(c) Incremental	CSA CCM covers Recovery Time Objective (RTO) but does not cover Recovery Point Objective (RPO). Cloud Service Providers shall define recovery and business resumption priorities for systems and applications.	Recovery Point Objective (RPO) is not explicitly mentioned in CSA CCM.
21.3 BCP and DR testing		
21.3.4(a) Incremental	CSA CCM does not define a specific frequency for the testing of business continuity plans. Cloud Service Providers shall ensure that business continuity and disaster recovery plans are tested and updated at least on an annual basis, and include plans for various test case scenarios (refer to MTCS SS Clause 21.3.4(a) for examples).	CSA CCM requires business continuity plans to be tested at planned intervals but does not specify the frequency of such tests.

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
22 Cloud services administration		
22.6 Password reset and first logon		
22.6.4(a) Incremental	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. Cloud Service Providers shall implement appropriate mechanism such that half of the new password is provided via an out-of-band mechanism directly to the affected person and the other half is provided to their supervisor.	CSA CCM does not specifically require that half of the new password be provided via an out-of-band mechanism directly to the affected person and the other half provided to their supervisor.
22.7 Administrator access security		
22.7.4(a) Incremental	CSA CCM does not specifically require the use of privilege access management tools. Cloud Service Providers shall implement privilege access management tools to restrict administrators' direct access to privileged functions and accounts.	While CSA CCM covers access management in general, it does not specifically require the use of privilege access management tools to restrict administrator's access to privileged functions and accounts.
22.10 Segregation of duties		
22.10.4(a) Incremental	CSA CCM does not specify a frequency for the reviews of access rights and segregation of duties. Cloud Service Providers shall conduct reviews for access rights and segregation of duties at least on a monthly basis.	While CSA CCM covers access rights review and segregation of duties, it does not specifically such review to be conducted on a monthly basis.
22.12 Third party administrative access		
22.12.4(a) Incremental	CSA CCM does not explicitly require that third party access to the environment shall be allowed only under the supervision of the Cloud Service Provider's personnel. The Cloud Service Provider shall only allow third party access to the environment under the direct supervision of the Cloud Service Provider's relevant personnel.	While policies and procedures on user access are mentioned, CSA CCM does not explicitly require that third party access to the environment be allowed only under the direct supervision of the Cloud Service Provider's relevant personnel.
22.13 Service and application accounts		
22.13.4(a) Incremental	CSA CCM does not cover the change of passwords for service accounts. Cloud Service Providers shall establish procedures to change service account passwords at least twice annually or when an administrator leaves the organisation.	While CSA CCM defines controls for user access policies and procedures, it does not cover the change of service account passwords.
23 Cloud user access		
23.2 User access security		
23.2.4(a) New	CSA CCM does not specifically require the restriction of storage of the same user identity in multiple environments. Cloud Service Providers shall not store same user identities in multiple cloud environments.	CSA CCM does not explicitly state utilisation of identity management to coordinate and restrict storage of same user identity in multiple cloud environments.
23.7 User session management		
23.7.4(a) Incremental	Cloud Service Providers shall establish and implement an appropriate maximum connection time of applications for all user sessions, based on approved hardening documents.	While CSA CCM defines controls pertaining to access control, it does not define connection time restrictions for applications.

MTCS clause	Implementation guidance	Additional context on gaps identified on CSA CCM
24 Tenancy and customer isolation		
24.1 Multi tenancy		
24.1.4(a) Incremental	Cloud Service Providers shall have monitoring mechanisms in place to detect when a virtual host attempts to access another virtual host.	While CSA CCM requires some form of intrusion detection to detect potentially suspicious network behaviors, it does not explicitly require the implementation of such monitoring mechanisms to detect a virtual host's attempt to access another virtual host.
24.5 Storage area networks (SAN)		
24.5.4(a) New	CSA CCM does not cover hard zones and Logical Unit Numbers (LUN). Cloud Service Providers shall leverage hard zones configured in the FC switch or similar controls. Where feasible, Cloud Service Providers shall also leverage Logical Unit Numbers (LUN) masking or similar controls on storage devices.	CSA CCM does not cover hard zones.
24.5.4(b) New		CSA CCM does not cover Logical Unit Numbers (LUN).
24.6 Data segregation		
24.6.4(b) Incremental	Cloud Service Provider shall have policies, procedural or technical measures in place to ensure that backups are segregated by users.	While CSA CCM states controls to segment user access, it does not explicitly cover the segregation of backups by cloud users.

<End of Implementation Guideline Report>