INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS) Gap Analysis 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 Gap Analysis Report is for general information purposes only. The Gap Analysis 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 Gap Analysis Report. The Working Group and IDA are entitled to add, delete or change any information in the Gap Analysis 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 Gap Analysis Report is the first 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 CSA STAR audit overlaps with scope of MTCS SS.

3 Intended Audience

This Gap Analysis 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.

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 – Approach
- Section 7 – Summary of Findings
- Section 8 – Tips on Using this Gap Analysis Report
- Section 9 – Gap Analysis

5 Terms and Definitions

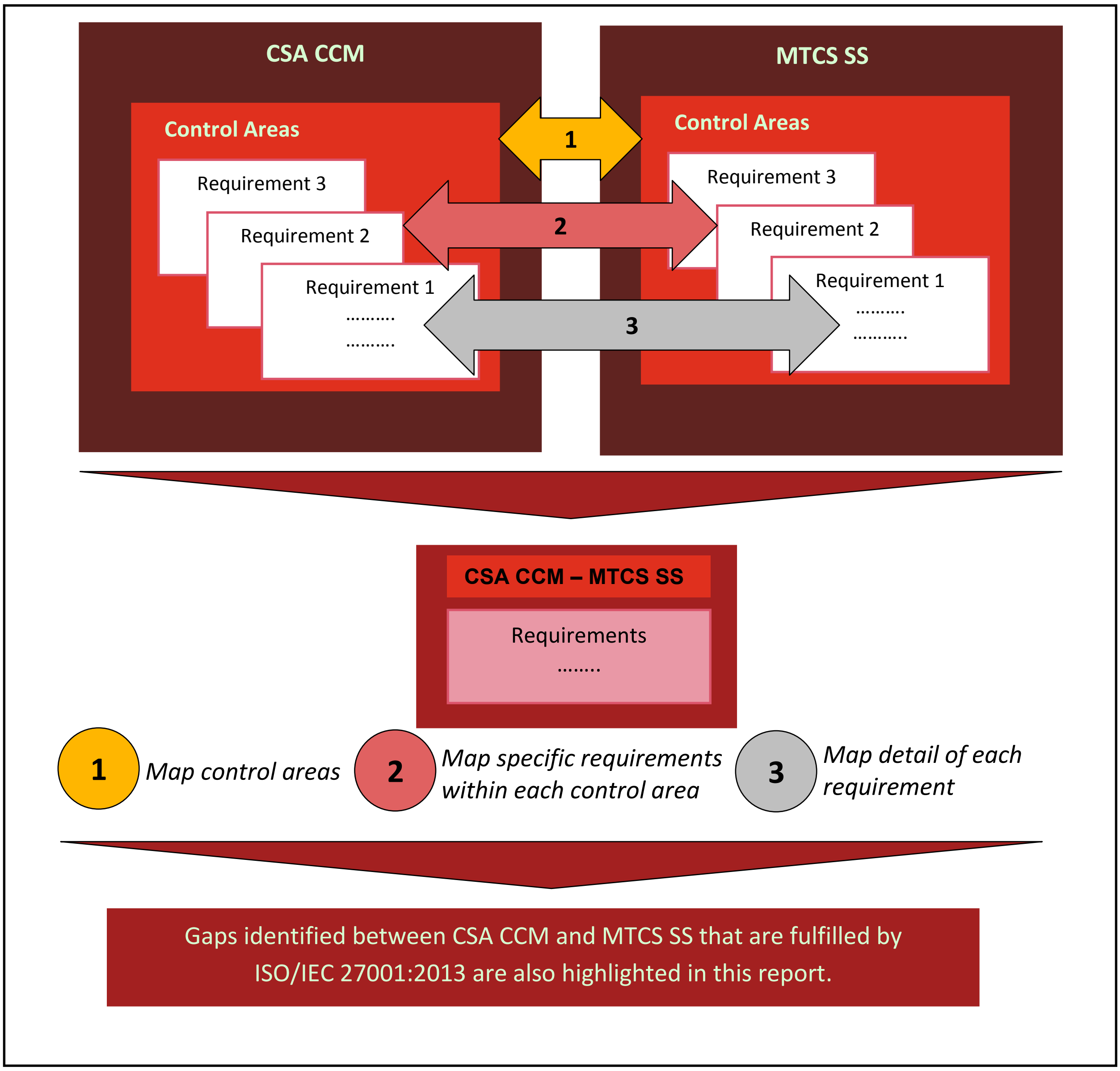
Cloud-related terms used in this report are defined in CSA CCM v3.0, MTCS SS and ISO/IEC 27001:2013.

6 Approach

In order to assist entities that are CSA STAR certified to adopt the MTCS SS, requirements listed in the MTCS SS were matched with equivalent requirements in CSA CCM. This followed a structured and systematic three (3) step approach:

- Map control areas
- Map specific requirements within control area
- Map details of each requirement

As the STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in CSA CCM, the gaps identified above that are fulfilled by ISO/IEC 27001:2013 are also highlighted in this report to provide further guidance.


CSA CCM
Control Areas
Requirement 3
Requirement 2
Requirement 1
……….
……….
MTCS SS
Control Areas
Requirement 3
Requirement 2
Requirement 1
……….
………..
1
2
3
CSA CCM – MTCS SS
Requirements
……..
1
Map control areas
2
Map specific requirements within each control area
3
Map detail of each requirement
Gaps identified between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 are also highlighted in this report.

7 Summary of Findings

The purpose of this summary section is to provide an overview of the differences between MTCS SS and CSA STAR categorised as follows:

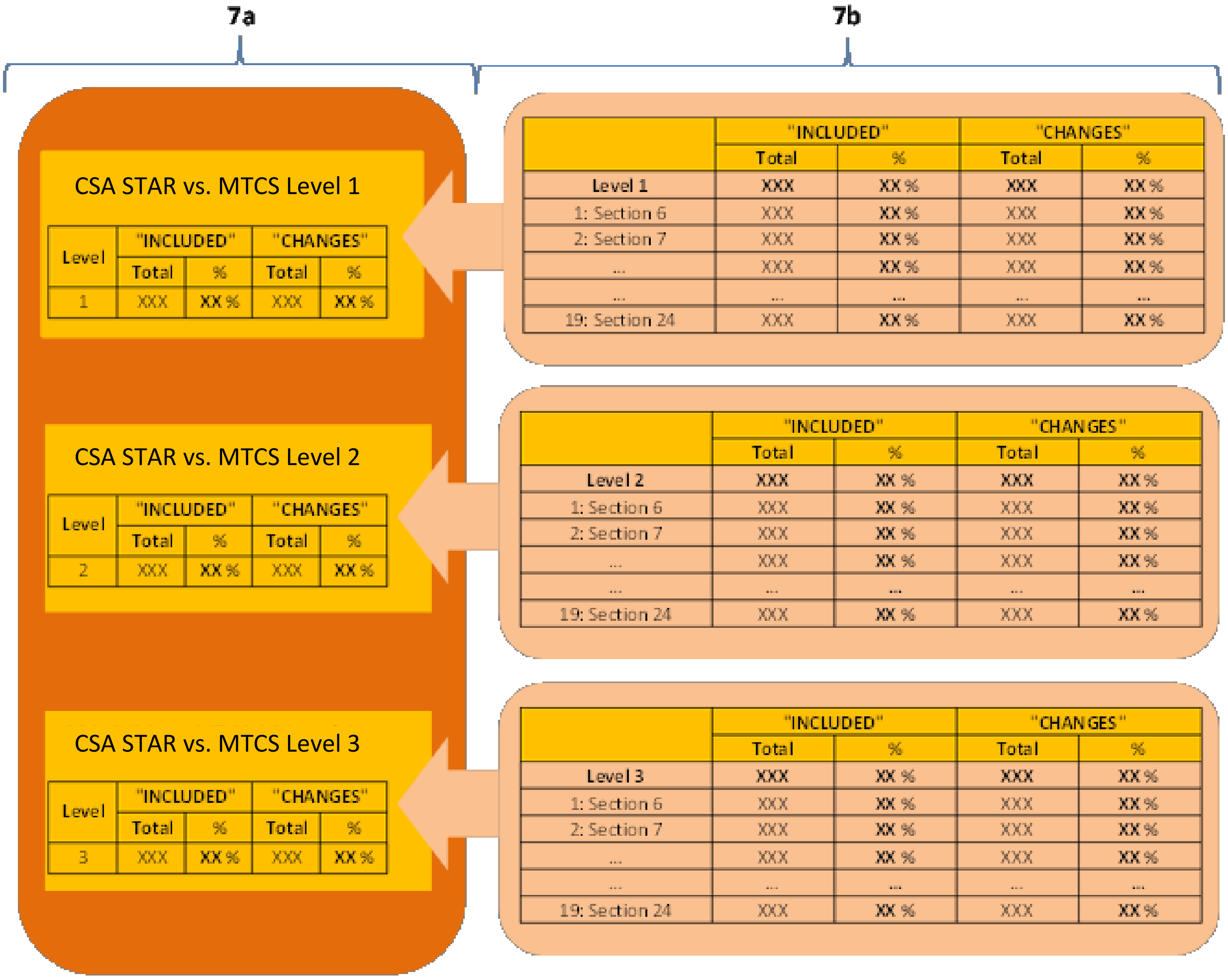
a. Summary by Level in MTCS SS certification (Levels 1, 2 and 3)

Section 7.1 summarises the total gaps identified for CSA CCM as compared to each of the three (3) levels of MTCS SS. As the STAR Certification is based upon achieving both ISO/IEC 27001 and CSA CCM, gaps that are fulfilled by ISO/IEC 27001 are also highlighted in this report.

b. Summary by Control Area in MTCS SS Levels 1, 2 and 3

Section 7.2 summarises the total gaps identified for CSA CCM as compared to each of the nineteen (19) areas for the three (3) levels in MTCS SS. Similar to the above, gaps that are fulfilled by ISO/IEC 27001 are also highlighted in this report.

The table structure for 7a and 7b is as follows:



CSA STAR vs. MTCS Level 1

Level	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
1	XXX	XX %	XXX	XX %

CSA STAR vs. MTCS Level 2

Level	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
2	XXX	XX %	XXX	XX %

CSA STAR vs. MTCS Level 3

Level	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
3	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 1	XXX	XX %	XXX	XX %
1: Section 6	XXX	XX %	XXX	XX %
2: Section 7	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
19: Section 24	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 2	XXX	XX %	XXX	XX %
1: Section 6	XXX	XX %	XXX	XX %
2: Section 7	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
19: Section 24	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 3	XXX	XX %	XXX	XX %
1: Section 6	XXX	XX %	XXX	XX %
2: Section 7	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
19: Section 24	XXX	XX %	XXX	XX %

Cloud Service Providers that are CSA STAR certified and are interested in obtaining MTCS certification can view the key areas that require enhancements / upgrades in order to adopt MTCS SS. Description of the respective columns are listed below:

Column	Column description
Total Clauses	Indicates the number of clauses currently listed in MTCS SS. The Total is inclusive of the preceding Level's requirements, for example, Level 3 includes requirements in Levels 1 and 2.
INCLUDED	Indicates the number of clauses in MTCS SS that are equally represented in CSA STAR[1].
CHANGES	Indicates the summation of "INCREMENTAL" and "NEW" clauses. Descriptions of the "INCREMENTAL" and "NEW" columns can be found in the following points.
INCREMENTAL	Indicates the number of clauses in MTCS SS that are stated with more detail 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 number of 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 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.

The colours green, yellow and red in the summary tables in Sections 7.1 and 7.2 denote the following:

- Green denotes >= 50% MTCS SS controls included in CSA STAR[1].
- Yellow denotes >= 20% and < 50% MTCS SS controls included in CSA STAR[1].
- Red denotes < 20% MTCS SS controls included in CSA STAR[1].

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

7.1 Summary by Level (Levels 1, 2 and 3)

The purpose of this summary by Level section is to provide an overview of the differences between MTCS SS and CSA STAR as grouped by MTCS SS certification Levels 1, 2 and 3. Cloud Service Providers that are CSA STAR certified and are interested in obtaining MTCS certification in a specific Level can view the effort required on identified enhancements / upgrades in order to adopt MTCS SS.

The table below provides a high level summary of the differences between MTCS SS Level 1 and CSA CCM. Cloud Service Providers looking to be cross certified to MTCS SS Level 1 can refer to this table for total requirements applicable to this level:

Level	Total Clauses	"INCLUDED"		"CHANGES" = “INCREMENTAL” + “NEW”		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 1	296	227	**77%**	69	**23%**	69	**23%**	0	**0%**

The table below provides a high level summary of the differences between MTCS SS Level 2 and CSA CCM. Cloud Service Providers looking to be cross certified to MTCS SS Level 2 can refer to this table for total requirements applicable to this level. Note that the total clauses of 449 comprise the 296 clauses in Level 1 and in addition, 153 unique Level 2 clauses.

Level	Total Clauses	"INCLUDED"		"CHANGES" = “INCREMENTAL” + “NEW”		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 2	449	327	**73%**	122	**27%**	116	**26%**	6	**1%**

The table below provides a high level summary of the differences between MTCS SS Level 3 and CSA CCM. Cloud Service Providers looking to be cross certified to MTCS SS Level 3 can refer to this table for total requirements applicable to this level. Note that the total clauses of 535 comprise the 449 clauses in Level 2 and in addition, 86 unique Level 3 clauses.

Level	Total Clauses	"INCLUDED"		"CHANGES" = “INCREMENTAL” + “NEW”		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 3	535	377	**70%**	158	**30%**	144	**27%**	14	**3%**

7.2 Summary by Control Areas

The purpose of this section is to provide an overview of the differences between MTCS SS and CSA STAR by Control Area in MTCS SS Levels 1, 2 and 3. Cloud Service Providers that are CSA STAR certified and are interested in obtaining MTCS certification in Levels 1, 2 or 3 can view the key logical areas that require enhancements / upgrades in order to adopt MTCS SS.

The table below summarises the differences between MTCS SS Level 1 and CSA CCM[1]:

Areas[2]	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	32	27	**84%**	5	**16%**	5	**16%**	0	**0%**
Section 7	10	10	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 8	8	7	**88%**	1	**13%**	1	**13%**	0	**0%**
Section 9	7	7	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 10	18	15	**83%**	3	**17%**	3	**17%**	0	**0%**
Section 11	17	16	**94%**	1	**6%**	1	**6%**	0	**0%**
Section 12	9	5	**56%**	4	**44%**	4	**44%**	0	**0%**
Section 13	13	13	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 14	23	19	**83%**	4	**17%**	4	**17%**	0	**0%**
Section 15	6	3	**50%**	3	**50%**	3	**50%**	0	**0%**
Section 16	15	12	**80%**	3	**20%**	3	**20%**	0	**0%**
Section 17	14	9	**64%**	5	**36%**	5	**36%**	0	**0%**
Section 18	27	22	**81%**	5	**19%**	5	**19%**	0	**0%**
Section 19	3	3	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 20	5	4	**80%**	1	**20%**	1	**20%**	0	**0%**
Section 21	11	11	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 22	34	20	**59%**	14	**41%**	14	**41%**	0	**0%**
Section 23	23	8	**35%**	15	**65%**	15	**65%**	0	**0%**
Section 24	21	16	**76%**	5	**24%**	5	**24%**	0	**0%**
Level 1	**296**	**227**	**77%**	**69**	**23%**	**69**	**23%**	**0**	**0%**

[1] The figures presented in the table may have a rounding variation of ±1%

[2] Requirements in MTCS SS are covered from Section 6 to Section 24 (19 areas). Cloud service providers should also note that they should accurately complete the Cloud Service Provider Disclosure as mentioned in Section 5 of MTCS SS.

The table below summarises the differences between MTCS SS Level 2 and CSA CCM[1]:

Areas[2]	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	40	34	**85%**	6	**15%**	6	**15%**	0	**0%**
Section 7	20	17	**85%**	3	**15%**	1	**5%**	2	**10%**
Section 8	16	14	**88%**	2	**13%**	2	**13%**	0	**0%**
Section 9	10	10	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 10	22	18	**82%**	4	**18%**	4	**18%**	0	**0%**
Section 11	24	23	**96%**	1	**4%**	1	**4%**	0	**0%**
Section 12	33	28	**85%**	5	**15%**	5	**15%**	0	**0%**
Section 13	22	20	**91%**	2	**9%**	2	**9%**	0	**0%**
Section 14	26	21	**81%**	5	**19%**	5	**19%**	0	**0%**
Section 15	8	3	**38%**	5	**63%**	5	**63%**	0	**0%**
Section 16	21	15	**71%**	6	**29%**	6	**29%**	0	**0%**
Section 17	22	11	**50%**	11	**50%**	11	**50%**	0	**0%**
Section 18	32	25	**78%**	7	**22%**	6	**19%**	1	**3%**
Section 19	9	9	**100%**	0	**0%**	0	**0%**	0	**0%**
Section 20	12	8	**67%**	4	**33%**	4	**33%**	0	**0%**
Section 21	13	12	**92%**	1	**8%**	1	**8%**	0	**0%**
Section 22	50	27	**54%**	23	**46%**	22	**44%**	1	**2%**
Section 23	32	11	**34%**	21	**66%**	21	**66%**	0	**0%**
Section 24	37	21	**57%**	16	**43%**	14	**38%**	2	**5%**
Level 2	**449**	**327**	**73%**	**122**	**27%**	**116**	**26%**	**6**	**1%**

[1] The figures presented in the table may have a rounding variation of ±1%

[2] Requirements in MTCS SS are covered from Section 6 to Section 24 (19 areas). Cloud service providers should also note that they should accurately complete the Cloud Service Provider Disclosure as mentioned in Section 5 of MTCS SS.

The table below summarises the differences between MTCS SS Level 3 and CSA CCM[1]:

Areas[2]	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	41	35	**85%**	6	**15%**	6	**15%**	0	**0%**
Section 7	24	18	**75%**	6	**25%**	3	**13%**	3	**13%**
Section 8	18	15	**83%**	3	**17%**	3	**17%**	0	**0%**
Section 9	17	16	**94%**	1	**6%**	1	**6%**	0	**0%**
Section 10	24	19	**79%**	5	**21%**	4	**17%**	1	**4%**
Section 11	29	27	**93%**	2	**7%**	1	**3%**	1	**3%**
Section 12	38	32	**84%**	6	**16%**	6	**16%**	0	**0%**
Section 13	27	24	**89%**	3	**11%**	2	**7%**	1	**4%**
Section 14	31	21	**68%**	10	**32%**	9	**29%**	1	**3%**
Section 15	11	3	**27%**	8	**73%**	8	**73%**	0	**0%**
Section 16	23	16	**70%**	7	**30%**	7	**30%**	0	**0%**
Section 17	23	11	**48%**	12	**52%**	12	**52%**	0	**0%**
Section 18	32	25	**78%**	7	**22%**	6	**19%**	1	**3%**
Section 19	25	24	**96%**	1	**4%**	1	**4%**	0	**0%**
Section 20	14	8	**57%**	6	**43%**	6	**43%**	0	**0%**
Section 21	20	16	**80%**	4	**20%**	4	**20%**	0	**0%**
Section 22	56	28	**50%**	28	**50%**	27	**48%**	1	**2%**
Section 23	34	11	**32%**	23	**68%**	22	**65%**	1	**3%**
Section 24	48	28	**58%**	20	**42%**	16	**33%**	4	**8%**
Level 3	**535**	**377**	**70%**	**158**	**30%**	**144**	**27%**	**14**	**3%**

[1] The figures presented in the table may have a rounding variation of ±1%

[2] Requirements in MTCS SS are covered from Section 6 to Section 24 (19 areas). Cloud service providers should also note that they should accurately complete the Cloud Service Provider Disclosure as mentioned in Section 5 of MTCS SS.

8 Tips on Using this Gap Analysis Report

The description of the respective columns in the gap analysis tables in Section 9 ‘Gap Analysis’ is listed below:

1) The column "MTCS Clause" specifies the clauses that are currently stated in MTCS SS.

2) The column "Gaps" indicates the following scenarios in the gap analysis, “INCLUDED”, “NEW” and “INCREMENTAL” as defined in Section 7 ‘Summary of Findings’.

3) The column “Reference to matching CSA CCM clauses” specifies the clauses that are currently stated in CSA CCM and have equal requirements or components relevant to the corresponding MTCS SS clause specified under the column “MTCS Clause”.

4) The column “Reference to matching CSA CCM sub-clauses” specifies the sub-clauses that are currently stated in CSA CCM and have equal requirements or components relevant to the corresponding MTCS SS clause specified under the column “MTCS Clause”. The corresponding parent clauses of these sub-clauses can be found under the column “Reference to matching CSA CCM clauses”.

5) The column "Remarks on identified gaps" denotes observations and additional notes based on the gap analysis:

Identified gaps between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 have the corresponding sections in ISO/IEC 27001:2013 listed in this column.

Note that requirements listed as “INCLUDED” will not be discussed further in subsequent documents (Implementation Guideline Report and Audit Checklist Report) as described in Section 2 ‘Purpose of Document’.

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 Section 15.1 ‘Vulnerability scanning’, Cloud Server Providers have to conduct vulnerability scanning more frequently if they are looking to be certified at the next level.

It is also recommended for Cloud Service Providers to view the complete set of requirements listed in the MTCS SS document for the authoritative list of requirements.

9 Gap Analysis

The purpose of this section is to list the differences between MTCS SS and CSA CCM describing gaps discovered in each control area and their respective clauses.

Identified gaps between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 have the corresponding sections in ISO/IEC 27001:2013 listed in the "Remarks on identified gaps" column.

9.1 Information security management

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
6 Information security management				
6.1 Information security management system (ISMS)				
6.1.2 Level 1 requirements				
6.1.2(a)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program	N.A
6.1.2(b)	INCLUDED	GRM Governance and Risk Management	GRM 04 -Management Program	N.A
6.1.2(c)	INCLUDED	GRM Governance and Risk Management	GRM 06 - Policy	N.A
6.1.2(d)	INCLUDED	GRM Governance and Risk Management	GRM 05 - Management Support / Involvement	N.A
6.1.2(e)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program GRM 08 - Policy Impact on Risk Assessments GRM 12 - Risk Mitigation / Acceptance	CSA CCM covers risk management process; however, it does not explicitly define risk relating to insiders.
6.1.2(f)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program GRM 03 - Management Oversight	N.A
6.1.2(g)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program	N.A
6.1.2(h)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
6.1.2(i)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program GRM 08 - Policy Impact on Risk Assessments GRM 10 - Risk Assessments	While CSA CCM covers risk management, it does not specify risk associated with cloud computing. However, CSA CCM is intended for cloud providers so this is considered included.
6.1.2(j)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 10 - VM Security - vMotion Data Protection IVS 05 - Vulnerability Management	CSA CCM does not require virtualisation specific controls in ISMS.
6.1.3 Level 2 requirements				
6.1.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 02 - Data Inventory / Flows	N.A
6.1.3(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability GRM Governance and Risk Management	STA 04 - Provider Internal Assessments GRM 08 - Policy Impact on Risk Assessments GRM 09 - Policy Reviews	N.A
6.1.4 Level 3 requirements				
6.1.4(a)	INCLUDED	N.A	N.A	CSA CCM requires the Cloud Service Provider to hold a certification for ISO / IEC 27001:2005 as a prerequisite.
6.2 Management of information security				
6.2.2 Level 1 requirements				
6.2.2(a)	INCLUDED	GRM Governance and Risk Management HRS Human Resources - Roles / Responsibilities	GRM 06 - Policy GRM 05 - Management Support / Involvement HRS 08 - Roles / Responsibilities	N.A
6.2.2(b)	INCLUDED	GRM Governance and Risk Management	GRM 05 - Management Support / Involvement	N.A
6.2.2(c)	INCLUDED	GRM Governance and Risk Management	GRM 05 - Management Support / Involvement GRM 04 - Management Program	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
6.2.2(d)	INCLUDED	STA Supply Chain Management, Transparency and Accountability IAM Identity & Access Management	STA 08 -Third Party Assessment STA 09 - Third Party Audits IAM 02 - Credential Lifecycle / Provision Management	N.A
6.2.3 Level 2 requirements				
6.2.3(a)	INCLUDED	GRM Governance and Risk Management	GRM 03 - Management Oversight	N.A
6.2.3(b)	INCLUDED	GRM Governance and Risk Management DSI Data Security & Information Lifecycle Management CCC Change Control & Configuration Management	GRM 04 - Management Program DSI 07 - Ownership / Stewardship CCC 01 -New Development / Acquisition	N.A
6.3 Management oversight of information security				
6.3.2 Level 1 requirements				
6.3.2(a)	INCLUDED	GRM Governance and Risk Management	GRM 03 - Management Oversight	While CSA CCM requires management to have an oversight of the information security program, it does not specifically require the board of directors to do so. Note: ISO/IEC 27001:2013 covers this requirement under Section 5.
6.3.2(b)	INCLUDED	GRM Governance and Risk Management	GRM 03 - Management Oversight GRM 05 - Management Support / Involvement	N.A
6.3.2(c)	INCLUDED	GRM Governance and Risk Management	GRM 11 - Risk Management Framework	N.A
6.4 Information security policy				
6.4.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
6.4.2(a)	INCLUDED	GRM Governance and Risk Management AIS Application & Interface Security AAC Audit Assurance & Compliance	GRM 06 - Policy AIS 04 - Data Security / Integrity AAC 03 - Information System Regulatory Mapping	N.A
6.4.2(b)	INCLUDED	GRM Governance and Risk Management HRS Human Resources	GRM 06 - Policy HRS 08 - Roles / Responsibilities	N.A
6.5 Review of information security policy				
6.5.2 Level 1 requirements				
6.5.2(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 09 - Policy Reviews	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.
6.5.3 Level 2 requirements				
6.5.3(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 09 - Policy Reviews	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.
6.6 Information security audits				
6.6.2 Level 1 requirements				
6.6.2(a)	INCREMENTAL	AAC Audit Assurance & Compliance	AAC 01 - Audit Planning	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	AAC Audit Assurance & Compliance	AAC 01 - Audit Planning	While CSA CCM covers the approval of audit plans by stakeholders, it does not specifically require the approval from an audit committee.
6.6.2(c)	INCLUDED	AAC Audit Assurance & Compliance	AAC 02 - Independent Audits	N.A
6.6.2(d)	INCLUDED	AAC Audit Assurance & Compliance	AAC 02 - Independent Audits	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
6.6.2(e)	INCLUDED	IAM Identity & Access Management	IAM 01 - Audit Tools Access	N.A
6.7 Information security liaisons (ISL)				
6.7.2 Level 1 requirements				
6.7.2(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 01 - Contact / Authority Maintenance	N.A
6.7.2(b)	INCLUDED	HRS Human Resources	HRS 05 - Industry Knowledge / Benchmarking	N.A
6.7.2(c)	INCLUDED	N.A	N.A	CSA CCM does not require subscription to vendor's security bulletins and alerts to ensure prompt implementation of security updates. Note: ISO/IEC 27001:2013 covers this requirement under Sections 5.2, 7.4 and A.6.1.
6.7.2(d)	INCLUDED	HRS Human Resources	HRS 05 - Industry Knowledge / Benchmarking	N.A
6.7.3 Level 2 requirements				
6.7.3(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
6.8 Acceptable Usage				
6.8.2 Level 1 requirements				
6.8.2(a)	INCLUDED	HRS Human Resources	HRS 09 - Technology Acceptable Use	N.A
6.8.2(b)	INCLUDED	HRS Human Resources	HRS 06 - Mobile Device Management HRS 09 - Technology Acceptable Use	N.A
6.8.2(c)	INCLUDED	HRS Human Resources MOS Mobile Security	HRS 09 - Technology Acceptable Use MOS 02 - Application Stores	N.A
6.8.3 Level 2 requirements				
6.8.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management HRS Human Resources MOS Mobile Security	DSI 04 - Handling / Labeling / Security Policy HRS 09 - Technology Acceptable Use MOS 02 - Application Stores	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
6.8.3(b)	INCLUDED	DCS Datacenter Security	DCS 04 - Off-Site Authorization DCS 03 - Equipment Identification	N.A

9.2 Human resources

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
7 Human resources				
7.1 Background screening				
7.1.2 Level 1 requirements				
7.1.2(a)	INCLUDED	HRS Human Resources	HRS 02 - Background Screening	N.A
7.1.2(b)	INCLUDED	HRS Human Resources	HRS 02 - Background Screening	N.A
7.1.3 Level 2 requirements				
7.1.3(a)	INCREMENTAL	HRS Human Resources	HRS 02 - Background Screening	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.
7.1.4 Level 3 requirements				
7.1.4(a)	INCREMENTAL	HRS Human Resources	HRS 02 - Background Screening	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				
7.2.3 Level 2 requirements				
7.2.3(a)	**NEW**	N.A	N.A	CSA CCM does not require annual evaluation of personnel with access to Cloud Service Management Network or Cloud Service Delivery Network.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
7.2.3(b)	**NEW**	N.A	N.A	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.
7.2.4 Level 3 requirements				
7.2.4(a)	**NEW**	N.A	N.A	CSA CCM does not specify controls to evaluate all personnel annually.
7.2.4(b)	INCLUDED	IAM Identity & Access Management	IAM 07 - Third Party Access	CSA CCM requires third-party access to the organization's information systems and data to be monitored, however, it does not specify controls to perform spot checks, re-briefing and maintenance of monitoring logs relating to access behaviors on critical systems and data for all personnel. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
7.3 Employment and contract terms and conditions				
7.3.2 Level 1 requirements				
7.3.2(a)	INCLUDED	GRM Governance and Risk Management HRS Human Resources	GRM 07 - Policy Enforcement HRS 11 - User Responsibility	N.A
7.3.2(b)	INCLUDED	HRS Human Resources	HRS 03 - Employment Agreements	N.A
7.3.2(b)	INCLUDED	HRS Human Resources	HRS 01 - Asset Returns	N.A
7.3.2(d)	INCLUDED	HRS Human Resources	HRS 03 - Employment Agreements	N.A
7.3.3 Level 2 requirements				
7.3.3(a)	INCLUDED	HRS Human Resources	HRS 04 - Employment Termination	

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
7.3.3(b)	INCLUDED	HRS Human Resources	HRS 01 - Asset Returns HRS 04 - Employment Termination	While CSA CCM defines that upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned, it does not state about developing an exit process. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.7.3 and A.8.1.
7.3.4 Level 3 requirements				
7.3.4(a)	INCREMENTAL	HRS Human Resources	HRS 03 - Employment Agreements	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.
7.4 Disciplinary process				
7.4.2 Level 1 requirements				
7.4.2(a)	INCLUDED	GRM Governance and Risk Management	GRM 07 - Policy Enforcement	N.A
7.5 Asset returns				
7.5.2 Level 1 requirements				
7.5.2(a)	INCLUDED	HRS Human Resources	HRS 01 - Asset Returns	N.A
7.6 Information security training and awareness				
7.6.2 Level 1 requirements				
7.6.2(a)	INCLUDED	HRS Human Resources	HRS 10 - Training / Awareness	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
7.6.2(b)	INCLUDED	HRS Human Resources	HRS 10 - Training / Awareness	While CSA CCM specifies that a general information security awareness program should be implemented, however, it does not specify implementation of an incident management focus training program. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2(b) and A.7.2.
7.6.3 Level 2 requirements				
7.6.3(a)	INCLUDED	HRS Human Resources	HRS 10 - Training / Awareness	N.A
7.6.3(b)	INCLUDED	HRS Human Resources GRM Governance and Risk Management	HRS 10 - Training / Awareness GRM 03 - Management Oversight	N.A
7.6.3(c)	INCLUDED	GRM Governance and Risk Management	GRM 03 - Management Oversight	N.A
7.6.3(d)	INCLUDED	HRS Human Resources GRM Governance and Risk Management	HRS 10 - Training / Awareness GRM 03 - Management Oversight	While CSA CCM defines controls to train employees on information security, however, it does not explicitly specify training on personal data related controls. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2(b) and A.7.2.
7.6.3(e)	INCLUDED	HRS Human Resources	HRS 10 - Training / Awareness	While CSA CCM specifies that a general information security awareness program should be implemented, however, it does not explicitly state that Computer Misuse Act should be part of it. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2(b) and A.7.2.

9.3 Risk management

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
8 Risk management				
8.1 Risk management program				
8.1.2 Level 1 requirements				
8.1.2(a)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program GRM 11 - Risk Management Framework	N.A
8.1.2(b)	INCLUDED	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 10 - Risk Assessments	N.A
8.1.2(c)	INCLUDED	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 10 - Risk Assessments	N.A
8.1.2(d)	INCLUDED	GRM Governance and Risk Management	GRM 12 - Risk Mitigation / Acceptance	While not explicitly stated in CSA CCM, a mitigation plan would typically include risk treatment plan associated activities required by MTCS SS.
8.1.2(e)	INCLUDED	GRM Governance and Risk Management	GRM 11 - Risk Management Framework GRM 12 - Risk Mitigation / Acceptance	N.A
8.1.3 Level 2 requirements				
8.1.3(a)	INCLUDED	GRM Governance and Risk Management	GRM 12 - Risk Mitigation / Acceptance	While CSA CCM covers acceptance of risks based on risk criteria, it does not specifically require the types of risk criteria as stated in MTCS SS. Note: ISO/IEC 27001:2013 covers this requirement under Section 6.1.2.
8.1.4 Level 3 requirements				
8.1.4(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 10 - Risk Assessments GRM 11 - Risk Management Framework GRM 12 - Risk Mitigation / Acceptance	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.
8.2 Risk assessment				
8.2.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
8.2.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience GRM Governance and Risk Management	BCR 09 - Impact Analysis GRM 10 - Risk Assessments	N.A
8.2.2(b)	INCREMENTAL	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 10 - 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.
8.2.2(c)	INCLUDED	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 10 - Risk Assessments	N.A
8.2.3 Level 2 requirements				
8.2.3(a)	INCLUDED	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 10 - Risk Assessments	While CSA CCM covers risk assessment in general, it does not specifically require these assessments to include data protection topics. Note: ISO/IEC 27001:2013 covers this requirement under Section 6.1.
8.3 Risk management				
8.3.3 Level 2 requirements				
8.3.3(a)	INCLUDED	GRM Governance and Risk Management	GRM 10 - Risk Assessments	N.A
8.3.3(b)	INCLUDED	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments	N.A
8.3.3(c)	INCLUDED	GRM Governance and Risk Management	GRM 03 - Management Oversight GRM 04 - Management Program	N.A
8.3.3(d)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program GRM 11 - Risk Management Framework GRM 12 - Risk Mitigation / Acceptance	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
8.3.3(e)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management SEF 05 - Incident Response Metrics	While CSA CCM requires the training of security-related events, it does not specifically require that risk assessments be check against in the event of an incident. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
8.3.4 Level 3 requirements				
8.3.4(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability AAC Audit Assurance & Compliance	STA 04 - Provider Internal Assessments AAC 01 - Audit Planning	While assessments of conformance and effectiveness of policies, procedures, and supporting measures and metrics are mentioned, CSA CCM does not explicitly require that IT risks metrics to be developed. Note: ISO/IEC 27001:2013 covers this requirement under Section 9.1.
8.4 Risk register				
8.4.3 Level 2 requirements				
8.4.3(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program GRM 12 - Risk Mitigation / Acceptance	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.

9.4 Third party

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
9 Third party				
9.1 Third party due diligence				
9.1.2 Level 1 requirements				
9.1.2(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 01 - Data Quality and Integrity STA 06 - Supply Chain Governance Reviews	N.A
9.1.2(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 01 - Data Quality and Integrity	N.A
9.2 Identification of risks related to third parties				
9.2.2 Level 1 requirements				
9.2.2(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
9.2.4 Level 3 requirements				
9.2.4(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements STA 06 - Supply Chain Governance Reviews STA 08 - Third Party Assessment STA 09 - Third Party Audits	N.A
9.2.4(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 01 - Data Quality and Integrity STA 06 - Supply Chain Governance Reviews STA 07 - Supply Chain Metrics	N.A
9.3 Third party agreement				
9.3.2 Level 1 requirements				
9.3.2(a)	INCLUDED	DSI Data Security & Information Lifecycle Management HRS Human Resources STA Supply Chain Management, Transparency and Accountability	DSI 02 - Data Inventory / Flows HRS 02 - Background Screening HRS 03 - Employment Agreements HRS 07 - Non-Disclosure Agreements STA 05 - Supply Chain Agreements STA 07 - Supply Chain Metrics	N.A
9.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
9.3.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management HRS Human Resources STA Supply Chain Management, Transparency and Accountability	DSI 02 - Data Inventory / Flows HRS 03 - Employment Agreements HRS 07 - Non-Disclosure Agreements STA 05 - Supply Chain Agreements STA 07 - Supply Chain Metrics	N.A
9.4 Third party delivery management				
9.4.2 Level 1 requirements				
9.4.2(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 08 - Third Party Assessment STA 09 - Third Party Audits	N.A
9.4.2(b)	INCLUDED	CCC Change Control & Configuration Management	CCC 05 - Production Changes	N.A
9.4.2(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 09 - Third Party Audits	N.A
9.4.3 Level 2 requirements				
9.4.3(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 01 - Data Quality and Integrity STA 03 - Network / Infrastructure Services STA 05 - Supply Chain Agreements STA 06 - Supply Chain Governance Reviews STA 07 - Supply Chain Metrics	N.A
9.4.3(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
9.4.4 Level 3 requirements				
9.4.4(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 09 - Third Party Audits	N.A
9.4.4(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 06 - Third Party Assessment STA 09 -Third Party Audits	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
9.4.4(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements STA 06 - Supply Chain Governance Reviews STA 07 - Supply Chain Metrics STA 08 - Third Party Assessment STA 09 - Third Party Audits	N.A
9.4.4(d)	INCREMENTAL	STA Supply Chain Management, Transparency and Accountability	STA 08 - Third Party Assessment STA 09 - Third Party Audits	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.
9.4.4(e)	INCLUDED	BCR Business Continuity Management & Operational Resilience STA Supply Chain Management, Transparency and Accountability	BCR 01 - Business Continuity Planning BCR 02 - Business Continuity Testing STA 05 - Supply Chain Agreements	N.A

9.5 Legal and compliance

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
10 Legal and compliance				
10.1 Compliance with regulatory and contractual requirements				
10.1.2 Level 1 requirements				
10.1.2(a)	INCLUDED	AAC Audit Assurance & Compliance DSI Data Security & Information Lifecycle Management	AAC 03 - Information System Regulatory Mapping DSI 01 - Classification	N.A
10.1.2(b)	INCLUDED	AAC Audit Assurance & Compliance AIS Application & Interface Security	AAC 03 - Information System Regulatory Mapping AIS 04 - Data Security / Integrity	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
10.1.2(c)	INCLUDED	AAC Audit Assurance & Compliance	AAC 03 - Information System Regulatory Mapping	N.A
10.1.2(d)	INCLUDED	AAC Audit Assurance & Compliance AIS Application & Interface Security	AAC 03 - Information System Regulatory Mapping AIS 04 - Data Security / Integrity	N.A
10.1.3 Level 2 requirements				
10.1.3(a)	INCLUDED	AAC Audit Assurance & Compliance GRM Governance and Risk Management	AAC 01 - Audit Planning GRM 06 - Policy	While CSA CCM specifies that security policies and procedures shall be reviewed and updated, it does not specify periodic review and update of the documentation for each category of information system elements. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
10.1.3(b)	INCLUDED	AIS Application & Interface Security HRS Human Resources	AIS 04 - Data Security / Integrity HRS 04 - Employment Termination	N.A
10.2 Compliance with policies and standards				
10.2.2 Level 1 requirements				
10.2.2(a)	INCLUDED	AAC Audit Assurance & Compliance STA Supply Chain Management, Transparency and Accountability	AAC 02 - Independent Audits AAC 03 - Information System Regulatory Mapping STA 04 - Provider Internal Assessments	N.A
10.2.3 Level 2 requirements				
10.2.3(a)	INCLUDED	AAC Audit Assurance & Compliance	AAC 02 - Independent Audits	N.A
10.2.4 Level 3 requirements				
10.2.4(a)	INCLUDED	AAC Audit Assurance & Compliance	AAC 01 - Audit Planning AAC 02 - Independent Audits	N.A
10.3 Prevention of misuse of cloud facilities				
10.3.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
10.3.2(a)	INCLUDED	HRS Human Resources	HRS 09 - Technology Acceptable Use	N.A
10.3.2(b)	INCREMENTAL	HRS Human Resources	HRS 10 - Training / Awareness	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(c)	INCLUDED	HRS Human Resources	HRS 10 - Training / Awareness	N.A
10.3.2(d)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	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.
10.3.2(e)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	While CSA CCM specifies information security controls to be included within the agreement, it does not explicitly mention inclusion of access and monitoring restrictions. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.15.1 and A.15.2.
10.4 Use of compliant cryptography controls				
10.4.2Level 1 requirements				
10.4.2(a)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation EKM 03 - Sensitive Data Protection EKM 04 - Storage and Access	While CSA CCM specifies controls to implement cryptography, it does not specify requirements to put in place relevant agreements. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.10.1, A.15.1 and A.15.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
10.4.2(b)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation EKM 03 - Sensitive Data Protection EKM 04 - Storage and Access	While CSA CCM specifies controls to implement encryption, it does not explicitly require knowledge of applicable laws and regulations in reference to cryptography. Note: ISO/IEC 27001:2013 covers this requirement under Section A.18.1.
10.4.2(c)	INCLUDED	EKM Encryption & Key Management	EKM 04 - Storage and Access	While CSA CCM specifies controls to implement cryptography, it does not specify requirements to put in place relevant agreements.
10.5 Third party compliance				
10.5.2 Level 1 requirements				
10.5.2(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 09 - Third Party Audits	N.A
10.5.2(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements STA 07 - Supply Chain Metrics	N.A
10.5.2(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
10.6 Continuous compliance monitoring				
10.6.2 Level 1 requirements				
10.6.2(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	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).
10.6.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	N.A
10.6.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
10.6.3(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines controls related to access control, it does not specify controls to provide system access reports within a defined timeframe.
10.6.4 Level 3 requirements				
10.6.4(a)	NEW	N.A	N.A	CSA CCM does not specify controls for real time monitoring.

9.6 Incident management

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
11 Incident management				
11.1 Information security incident response plan and procedures				
11.1.2 Level 1 requirements				
11.1.2(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 03 - Incident Reporting	N.A
11.1.2(b)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 01 - Contact / Authority Maintenance SEF 04 - Incident Response Legal Preparation	N.A
11.1.2(c)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 03 - Incident Reporting STA 05 - Supply Chain Agreements	N.A
11.1.2(d)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 04 - Incident Response Legal Preparation SEF 05 - Incident Response Metrics	While CSA CCM defines controls for incident management, it does not state controls to perform root cause and impact analysis of the incidents. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
11.1.2(e)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 01 - Contact / Authority Maintenance SEF 02 - Incident Management SEF 03 - Incident Reporting	While CSA CCM defines controls for incident management, it does not cover all recovery procedure and resolution timeframe. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.1.2(f)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 05 - Incident Response Metrics	N.A
11.1.2(g)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 03 - Incident Reporting	While CSA CCM defines controls for incident management, it does not state controls to classify incidents. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.1.2(h)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 02 - Incident Reporting	N.A
11.1.2(i)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management SEF 04 - Incident Response Legal Preparation	N.A
11.1.3 Level 2 requirements				
11.1.3(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 01 - Contact / Authority Maintenance SEF 03 - Incident Reporting	N.A
11.1.3(b)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 03 - Incident Reporting	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
11.1.3(c)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management	While CSA CCM specifies controls to manage incidents as per the process, it does not explicitly state that incidents have to be monitored and tracked to closure. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.1.3(d)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management	While CSA CCM specifies controls to manage incidents as per the process, it does not explicitly define controls for escalation. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.1.3(e)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics STA Supply Chain Management, Transparency and Accountability	SEF 02 - Incident Management STA 02 - Incident Reporting	While CSA CCM specifies controls to manage and report the incidents as per the process, it does not explicitly state that remediation plan should also be communicated to the customers. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.1.4 Level 3 requirements				
11.1.4(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	N.A
11.1.4(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability SEF Security Incident Management, E-Discovery & Cloud Forensics	STA 01 - Data Quality and Integrity STA 05 - Supply Chain Agreements SEF 02 - Incident Management	While CSA CCM mentions communication and notification for incidents, it does not explicitly include pre-determined plan to address public relations issues. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
11.1.4(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 01 - Data Quality and Integrity STA 05 - Supply Chain Agreements	While CSA CCM mentions communication and notification for incidents, it does not explicitly specify reporting of all major incidents in a chronological order to affected customers, the impact and preventive measures. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.1.4(d)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 04 - Incident Response Legal Preparation	N.A
11.2 Information security incident response plan testing and updates				
11.2.2 Level 1 requirements				
11.2.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 02 - Business Continuity Testing	CSA CCM mentions general controls related to incident management, it does not specify specific tests, scope and parties to be involved. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.2.2(b)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 02 - Business Continuity Testing	While CSA CCM mentions general controls related to incident management including testing at planned intervals, it does not specify testing to be conducted annually.
11.2.2(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 11 - Policy	CSA CCM mentions general controls related to incident management training, it does not specify specific responsibilities as part of training. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2(b), A.7.2 and A.16.1.
11.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
11.2.3(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management	CSA CCM mentions general controls related to incident management, it does not specify that incident response plan must be maintained up-to-date in accordance with industry standards. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.2.4 Level 3 requirements				
11.2.4(a)	NEW	N.A	N.A	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.
11.3 Information security incident reporting				
11.3.2 Level 1 requirements				
11.3.2(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 03 - Incident Reporting	N.A
11.3.2(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 02 - Incident Reporting	N.A
11.4 Problem management				
11.4.2 Level 1 requirements				
11.4.2(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management	While CSA CCM mentions policies and procedures related to incident management, it does not specify requirements specific to problem management and prioritisation. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
11.4.2(b)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management	While CSA CCM mentions policies and procedures related to incident management, it does not specify requirements specific to problem management and roles and responsibilities. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.6.1, A.7.2 and A.16.1.
11.4.2(c)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 02 - Incident Management	While CSA CCM mentions policies and procedures related to incident management, it does not specify requirements specific to problem management, escalation and severity levels. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
11.4.3 Level 2 requirements				
11.4.3(a)	INCLUDED	SEF Security Incident Management, E-Discovery & Cloud Forensics	SEF 05 - Incident Response Metrics	N.A

9.7 Data governance

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
12 Data governance				
12.1 Data classification				
12.1.3 Level 2 requirements				
12.1.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 01 - Classification DSI 02 - Data Inventory / Flows DSI 03 - eCommerce Transactions DSI 04 - Handling / Labeling / Security Policy	N.A
12.1.3(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 01 - Classification DSI 04 - Handling / Labeling / Security Policy	N.A
12.1.3(c)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 01 - Classification DSI 03 - eCommerce Transactions EKM 03 - Sensitive Data Protection	N.A
12.2 Data ownership				
12.2.3 Level 2 requirements				
12.2.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 07 - Ownership / Stewardship	N.A
12.3 Data integrity				
12.3.3 Level 2 requirements				
12.3.3(a)	INCLUDED	AIS Application & Interface Security	AIS 03 - Data Integrity AIS 04 - Data Security / Integrity	N.A
12.3.3(b)	INCLUDED	AIS Application & Interface Security	AIS 03 - Data Integrity AIS 04 - Data Security / Integrity	N.A
12.4 Data labelling / handling				
12.4.2 Level 1 requirements				
12.4.2(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 04 - Handling / Labeling / Security Policy	N.A
12.4.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
12.4.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 02 - Data Inventory / Flows DSI 04 - Handling / Labeling / Security Policy	N.A
12.4.3(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 02 - Data Inventory / Flows DSI 04 - Handling / Labeling / Security Policy	N.A
12.4.3(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability DSI Data Security & Information Lifecycle Management	STA 05 - Supply Chain Agreements DSI 02 - Data Inventory / Flows	N.A
12.4.4 Level 3 requirements				
12.4.4(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability DSI Data Security & Information Lifecycle Management	STA 05 - Supply Chain Agreements DSI 02 - Data Inventory / Flows	N.A
12.4.4(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 04 - Handling / Labeling / Security Policy	While data labeling and handling controls are mentioned in CSA CCM, it does not define the procedures on handling of data upon termination of service. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
12.5 Data protection				
12.5.2 Level 1 requirements				
12.5.2(a)	INCREMENTAL	IAM Identity & Access Management DSI Data Security & Information Lifecycle Management	IAM 02 - Credential Lifecycle / Provision Management DSI 02 - Data Inventory / Flows DSI 08 - Secure Disposal	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.
12.5.2(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 02 - Data Inventory / Flows DSI 08 - Secure Disposal	N.A
12.5.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
12.5.3(a)	INCLUDED	GRM Governance and Risk Management STA Supply Chain Management, Transparency and Accountability	GRM 02 - Data Focus Risk Assessments GRM 04 - Management Program STA 04 - Provider Internal Assessments	N.A
12.5.3(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 05 - Information Leakage	N.A
12.5.3(c)	INCLUDED	EKM Encryption & Key Management MOS Mobile Security	EKM 04 - Storage and Access MOS 11 - Encryption	N.A
12.5.3(d)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 02 - Change Detection	N.A
12.5.4 Level 3 requirements				
12.5.4(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 04 - Management Program	While policies and procedures to prevent data loss and destruction are mentioned, CSA CCM does not define a specific data loss prevention strategy.
12.6 Data retention				
12.6.3 Level 2 requirements				
12.6.3(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	N.A
12.6.3(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	N.A
12.6.3(c)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 08 - Secure Disposal	N.A
12.6.3(d)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	While CSA CCM defines data retention requirements, it does not specify deletion of data beyond retention period.
12.6.3(e)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	N.A
12.6.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
12.6.4(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
12.6.4(b)	INCLUDED	DSI Data Security & Information Lifecycle Management BCR Business Continuity Management & Operational Resilience	DSI 01 - Classification BCR 12 - Retention Policy	N.A
12.7 Data backups				
12.7.2 Level 1 requirements				
12.7.2(a)	INCREMENTAL	DSI Data Security & Information Lifecycle Management	DSI 04 - Handling / Labeling / Security Policy	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(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	N.A
12.7.2(c)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	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 Level 1 requirements				
12.8.2(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 08 - Secure Disposal	N.A
12.8.2(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 08 - Secure Disposal	N.A
12.8.2(c)	INCREMENTAL	GRM Governance and Risk Management DSI Data Security & Information Lifecycle Management	GRM 02 - Data Focus Risk Assessments DSI 08 - 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.
12.9 Secure disposal verification of live instances and backups				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
12.9.3 Level 2 requirements				
12.9.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 08 - Secure Disposal	N.A
12.10 Tracking of data				
12.10.3 Level 2 requirements				
12.10.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 02 - Data Inventory / Flows	N.A
12.11 Tracking of data				
12.11.3 Level 2 requirements				
12.11.3(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 06 - Non-Production Data	N.A
12.11.3(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 06 - Non-Production Data	N.A
12.11.3(c)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 06 - Non-Production Data	N.A
12.11.3(d)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 06 - Non-Production Data	N.A

9.8 Audit logging and monitoring

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.1 Audit logging and monitoring				
13.1.2 Level 1 requirements				
13.1.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	N.A
13.1.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	N.A
13.1.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 02 - Change Detection	N.A
13.1.2(d)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	N.A
13.1.2(e)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM requires audit logging to detect anomalies, it does not specifically require that such audit trails be reviewed regularly. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.1.2(f)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM requires audit logging to detect anomalies, it does not explicitly state review logging of identification and authentication mechanism usage, and initializing of audit trail files. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.1.2(g)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 03 - Clock Synchronization	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.1.2(h)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM defines monitoring controls, it does not specify monitoring the use of information processing facilities. Note: ISO/IEC 27001:2013 covers this requirement under Sections 9.1, 9.3 and A.12.4.
13.1.3 Level 2 requirements				
13.1.3(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 07 - OS Hardening and Base Controls	While CSA CCM requires audit logging, it does not specifically require that audit trails be enabled for all users' access on all system and network components in the cloud environment. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.1.3(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM requires audit logging to detect anomalies, it does not specifically require attempts of invalid logical access to be logged. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.1.3(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 07 - OS Hardening and Base Controls	While CSA CCM requires audit logging, it does not specifically require audit trails to be enabled for creation and deletion of system-level objects. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.1.3(d)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 02 - Change Detection IVS 07 - OS Hardening and Base Controls	N.A
13.1.3(e)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 06 - Network Security	N.A
13.1.4 Level 3 requirements				
13.1.4(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 06 - Network Security	N.A
13.1.4(b)	INCLUDED	CCC Change Control & Configuration Management IVS Infrastructure & Virtualization Security	CCC 04 - Unauthorized Software Installations IVS 02 - Change Detection	N.A
13.1.4(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 02 - Change Detection	N.A
13.1.4(d)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 02 - Change Detection	While CSA CCM requires that alerts be raised for erratic system behaviour or unusual activities, it does not explicitly require such alerts to be followed up, verified and addressed. Note: ISO/IEC 27001:2013 covers this requirement under Section A.16.1.
13.2 Log review				
13.2.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.2.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	CSA CCM does not require log review. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.2.3 Level 2 requirements				
13.2.3(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 06 - Network Security	CSA CCM does not explicitly require log reviews to include all critical systems and services performing security functions.
13.2.4 Level 3 requirements				
13.2.4(a)	NEW	N.A	N.A	CSA CCM does not require an automated tool for real time monitoring of logs.
13.3 Audit trails				
13.3.2 Level 1 requirements				
13.3.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM requires the use of audit logs and audit trails, it does not specify details to be captured in such audit logs and audit trails. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.3.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM defines controls related to audit logs and audit trails, however it does not explicitly restrict access to audit trails. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.3.3(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM covers audit logs and audit trails in general, it does not specify that such audit logs and audit trails be written to write-only media or a tamper resistant location. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.4 Backup and retention of audit trails				
13.4.2 Level 1 requirements				
13.4.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	N.A
13.4.3 Level 2 requirements				
13.4.3(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM covers the lifecycle management of audit logs and restricting access of such logs to authorised personnel, it does not require that such audit logs be backed up regularly. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.4.
13.4.3(b)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	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.
13.5 Usage logs				
13.5.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.5.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection	While CSA CCM covers the lifecycle management of audit logs in general, it does not specifically require that such logs shall have strict file and directory permissions.

9.9 Secure configuration

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
14 Secure configuration				
14.1 Server and network device configuration standards				
14.1.2 Level 1 requirements				
14.1.2(a)	INCLUDED	CCC Change Control & Configuration Management GRM Governance and Risk Management	CCC 05 - Production Changes GRM 01 - Baseline Requirements	N.A
14.1.2(b)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	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(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls IVS 11 - VMM Security - Hypervisor Hardening	N.A
14.1.2(d)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	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.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
14.1.2(e)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	While CSA CCM has defined configuration controls, it does not explicitly require clipboard or file-sharing services to be disabled.
14.1.4 Level 3 requirements				
14.1.4(a)	NEW	N.A	N.A	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				
14.2.2 Level 1 requirements				
14.2.2(a)	INCLUDED	CCC Change Control & Configuration Management TVM Threat and Vulnerability Management	CCC 02 - Outsourced Development TVM 03 - Mobile Code	N.A
14.2.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 01 - Anti-Virus / Malicious Software	N.A
14.2.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 01 - Anti-Virus / Malicious Software	While CSA CCM requires the use of anti-malware programs, it does not specifically require the assurance that these programs are effective for its purpose. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
14.2.2(d)	INCLUDED	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 01 - Anti-Virus / Malicious Software	While CSA CCM specifies installation of anti-malware programs, it does not explicitly state that controls should be implemented to ensure that such programs are running and are generating audit trails. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.2.
14.2.2(e)	INCREMENTAL	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 01 - Anti-Virus / Malicious Software	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.
14.2.2(f)	INCLUDED	CCC Change Control & Configuration Management IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	CCC 05 - Production Changes IVS 07 - OS Hardening and Base Controls TVM 01 - Anti-Virus / Malicious Software	While CSA CCM requires the use of anti-malware programs, it does not specifically require that any updates of the anti-malware programs (e.g., signatures, engines) have the ability to be rolled-back or mitigated in the event that the update causes system malfunctions. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.2.
14.2.2(g)	INCLUDED	GRM Governance and Risk Management HRS Human Resources	GRM 03 - Management Oversight HRS 10 - Training / Awareness HRS 11 - User Responsibility	N.A
14.2.4 Level 3 requirements				
14.2.4(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 01 - Anti-Virus / Malicious Software	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.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
14.2.4(b)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 02 - Outsourced Development	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.
14.3 Portable code				
14.3.2 Level 1 requirements				
14.3.2(a)	INCLUDED	TVM Threat and Vulnerability Management	TVM 03 - Mobile Code	N.A
14.4 Physical port protection				
14.4.2 Level 1 requirements				
14.4.2(a)	INCLUDED	DCS Datacenter Security IAM Identity & Access Management	DCS 02 - Controlled Access Points DCS 09 - User Access IAM 03 - Diagnostic / Configuration Ports Access	N.A
14.4.2(b)	INCLUDED	DCS Datacenter Security	DCS 09 - User Access	While CSA CCM defines physical security controls, it does not state that all unused physical and / or logical ports must be disabled. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.1.
14.4.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	While CSA CCM defines configuration controls, it does not require the configuration of unused physical and / or logical ports to be removed and any configuration for hardening to be applied. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.1.
14.5 Restrictions to system utilities				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
14.5.2 Level 1 requirements				
14.5.2(a)	INCLUDED	IAM Identity & Access Management	IAM 13 - Utility Programs Access	N.A
14.6 System and network session management				
14.6.2 Level 1 requirements				
14.6.2(a)	INCLUDED	HRS Human Resources	HRS 12 - Workspace	N.A
14.7 Unnecessary service and protocols				
14.7.2 Level 1 requirements				
14.7.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	N.A
14.7.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	N.A
14.7.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	N.A
14.7.3 Level 2 requirements				
14.7.3(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	N.A
14.8 Unauthorised software				
14.8.2 Level 1 requirements				
14.8.2(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 04 - Unauthorized Software Installations	N.A
14.9 Enforcement checks				
14.9.2 Level 1 requirements				
14.9.2(a)	INCLUDED	GRM Governance and Risk Management	GRM 01 - Baseline Requirements	N.A
14.9.3 Level 2 requirements				
14.9.3(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 01 - Baseline Requirements	CSA CCM requires checks to be performed annually instead of on a weekly basis.
14.9.3(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	N.A
14.9.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
14.9.4(a)	INCREMENTAL	GRM	GRM 01 - Baseline Requirements	CSA CCM requires checks to be performed annually instead of on a daily basis.
14.9.4(b)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	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.

9.10 Security testing and monitoring

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
15 Security testing and monitoring				
15.1 Vulnerability scanning				
15.1.2 Level 1 requirements				
15.1.2(a)	INCREMENTAL	CCC Change Control & Configuration Management GRM Governance and Risk Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing GRM-10 - Risk Assessments TVM 02 - Vulnerability / Patch Management	CSA CCM requires that vulnerability scanning be performed at least on an annual basis instead of a quarterly basis.
15.1.2(b)	INCREMENTAL	CCC Change Control & Configuration Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing TVM 02 - Vulnerability / Patch Management	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.
15.1.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
15.1.3(a)	INCREMENTAL	CCC Change Control & Configuration Management GRM Governance and Risk Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing GRM-10 - Risk Assessments TVM 02 - Vulnerability / Patch Management	CSA CCM requires that vulnerability scanning be performed at least on an annual basis instead of a quarterly basis or when significant changes occur to the environment.
15.1.3(b)	INCREMENTAL	CCC Change Control & Configuration Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing TVM 02 - Vulnerability / Patch Management	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.
15.1.4 Level 3 requirements				
15.1.4(a)	INCREMENTAL	CCC Change Control & Configuration Management GRM Governance and Risk Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing GRM-10 - Risk Assessments TVM 02 - Vulnerability / Patch Management	CSA CCM requires that vulnerability scanning be performed at least on an annual basis instead of a monthly basis.
15.2 Penetration testing				
15.2.2 Level 1 requirements				
15.2.2(a)	INCREMENTAL	CCC Change Control & Configuration Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing TVM 02 - Vulnerability / Patch Management	CSA CCM does not specify a frequency for conducting penetration tests.
15.2.4 Level 3 requirements				
15.2.4(a)	INCREMENTAL	CCC Change Control & Configuration Management TVM Threat and Vulnerability Management	CCC 03 - Quality Testing TVM 02 - Vulnerability / Patch Management	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				
15.3.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
15.3.2(a)	INCLUDED	GRM Governance and Risk Management TVM Threat and Vulnerability Management	GRM 08 - Policy Impact on Risk Assessments TVM 02 - Vulnerability / Patch Management	N.A
15.3.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 06 - Network Security	N.A
15.3.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 06 - Network Security	N.A
15.3.4 Level 3 requirements				
15.3.4(a)	INCREMENTAL	AAC Audit Assurance & Compliance CCC Change Control & Configuration Management TVM Threat and Vulnerability Management	AAC-02 - Independent Audits CCC 03 - Quality Testing TVM 02 - Vulnerability / Patch Management	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.

9.11 System acquisitions and development

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
16 System acquisitions and development				
16.1 Development, acquisition and release management				
16.1.2 Level 1 requirements				
16.1.2(a)	INCLUDED	AIS Application & Interface Security TVM Threat and Vulnerability Management	AIS 01 - Application Security TVM 02 - Vulnerability / Patch Management	N.A
16.1.2(b)	INCREMENTAL	AIS Application & Interface Security	AIS 01 - Application Security	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(c)	INCLUDED	AIS Application & Interface Security	AIS 01 - Application Security	While CSA CCM requires applications to be developed as per industry standards, it does not explicitly require the removal of test data and accounts before production systems become active. Note: ISO/IEC 27001:2013 covers this requirement under Section A.14.3.
16.1.2(d)	INCLUDED	AIS Application & Interface Security CCC Change Control & Configuration Management IPY Interoperability & Portability	AIS 01 - Application Security CCC 01 - New Development / Acquisition CCC 02 - Outsourced Development CCC 03 - Quality Testing IPY 01 - APIs IPY 03 - Policy & Legal	N.A
16.1.2(e)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security IVS 08 - Production / Non-Production Environments	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
16.1.2(f)	INCLUDED	CCC Change Control & Configuration Management	CCC 05 - Production Changes	N.A
16.1.2(g)	INCLUDED	CCC Change Control & Configuration Management	CCC 03 - Quality Testing	N.A
16.1.2(h)	INCLUDED	CCC Change Control & Configuration Management	CCC 03 - Quality Testing	N.A
16.1.2(i)	INCLUDED	AIS Application & Interface Security	AIS 03 - Data Integrity AIS 04 - Data Security / Integrity	N.A
16.1.2(j)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 01 - New Development / Acquisition CCC 02 - Outsourced Development	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	CCC Change Control & Configuration Management	CCC 01 - New Development / Acquisition CCC 02 - Outsourced Development	While CSA CCM requires ongoing source code review, it does not specifically require verification methods (e.g., checksum) to establish its authenticity.
16.1.2(l)	INCLUDED	CCC Change Control & Configuration Management	CCC 02 - Outsourced Development CCC 04 - Unauthorized Software Installations	N.A
16.1.3 Level 2 requirements				
16.1.3(a)	INCREMENTAL	AIS Application & Interface Security	AIS 04 - Data Security / Integrity	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.
16.1.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
16.1.4(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 02 - Outsourced Development CCC 03 - Quality Testing CCC 05 - Production Changes	While CSA CCM requires ongoing source code review and the quality testing of applications, it does not specifically require regular reviews of custom code prior to release to production. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.14.1 and A.14.2.
16.2 Web application security				
16.2.3 Level 2 requirements				
16.2.3(a)	INCREMENTAL	AIS Application & Interface Security CCC Change Control & Configuration Management	AIS 01 - Application Security CCC 03 - Quality Testing	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(b)	INCLUDED	N.A	N.A	CSA CCM does not require the installation of a web-application firewall or similar mechanism to detect and block web application vulnerability exploits in front of public-facing web applications. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.1.
16.2.3(c)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 03 - Quality Testing	While CSA CCM defines testing controls, it does not specifically cover public servers or the inclusion of public web services in security testing.
16.2.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
16.2.4(a)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 03 - Quality Testing	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.
16.3 System testing				
16.3.2 Level 1 requirements				
16.3.2(a)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 06 - Non-Production Data	CSA CCM does not require the installation of a web-application firewall or similar mechanism to detect and block web application vulnerability exploits in front of public-facing web applications. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.1.
16.3.3 Level 2 requirements				
16.3.3(a)	INCLUDED	CCC Change Control & Configuration Management DSI Data Security & Information Lifecycle Management	CCC 02 - Outsourced Development CCC 03 - Quality Testing CCC 05 - Production Changes DSI 06 - Non-Production Data	N.A
16.4 Source code security				
16.4.2 Level 1 requirements				
16.4.2(a)	INCLUDED	IAM Identity & Access Management	IAM 06 - Source Code Access Restriction	N.A
16.5 Outsourced software development				
16.5.2Level 1 requirements				
16.5.2(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 02 - Outsourced Development CCC 03 - Quality Testing	N.A
16.5.3 Level 2 requirements				
16.5.3(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 02 - Outsourced Development	N.A

9.12 Encryption

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
17 Encryption				
17.1 Encryption policies and procedures				
17.1.2 Level 1 requirements				
17.1.2(a)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation	N.A
17.1.2(b)	INCLUDED	EKM Encryption & Key Management	EKM 03 - Sensitive Data Protection	N.A
17.2 Channel encryption				
17.2.2 Level 1 requirements				
17.2.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	N.A
17.2.2(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 03 - eCommerce Transactions	N.A
17.3 Key management				
17.3.2 Level 1 requirements				
17.3.2(a)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation EKM 03 - Sensitive Data Protection	N.A
17.3.2(b)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation	N.A
17.3.2(c)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation	N.A
17.3.2(d)	INCREMENTAL	EKM Encryption & Key Management	EKM 01 - Entitlement	CSA CCM specifies controls to designate key custodians; however, it does not specify controls for obtaining formal acknowledgement of responsibilities from them.
17.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
17.3.3(a)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation	While CSA CCM states that policies and procedures shall be established for the management of cryptographic keys, it does not explicitly state that access should be restricted to minimise the number of custodians. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.9.2, A.9.4 and A.10.1.
17.3.3(b)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation	N.A
17.3.3(c)	NEW	N.A	N.A	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	EKM Encryption & Key Management	EKM 02 - Key Generation	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	EKM Encryption & Key Management	EKM 02 - Key Generation	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	EKM Encryption & Key Management	EKM 02 - Key Generation	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.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
17.3.3(g)	INCREMENTAL	EKM Encryption & Key Management	EKM 02 - Key Generation	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.
17.3.3(h)	INCREMENTAL	EKM Encryption & Key Management	EKM 02 - Key Generation	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.
17.3.4 Level 3 requirements				
17.3.4(a)	INCREMENTAL	EKM Encryption & Key Management	EKM 02 - Key Generation	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.
17.4 Electronic messaging security				
17.4.2 Level 1 requirements				
17.4.2(a)	INCLUDED	AIS Application & Interface Security EKM Encryption & Key Management	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection	While CSA CCM mentions general information security controls, it does not define controls for electronic messaging. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.2.
17.4.2(b)	INCLUDED	AIS Application & Interface Security EKM Encryption & Key Management	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection	While CSA CCM mentions general information security controls, it does not define controls for electronic messaging. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
17.4.2(c)	INCREMENTAL	AIS Application & Interface Security EKM Encryption & Key Management	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection	While CSA CCM mentions general information security controls, it does not define specific controls for electronic messaging.
17.4.2(d)	INCREMENTAL	AIS Application & Interface Security EKM Encryption & Key Management	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection	While CSA CCM mentions general information security controls, it does not define specific controls for electronic messaging.
17.4.2(e)	INCREMENTAL	AIS Application & Interface Security EKM Encryption & Key Management	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection	While CSA CCM mentions general information security controls, it does not define specific controls for electronic messaging.
17.4.2(f)	INCREMENTAL	AIS Application & Interface Security EKM Encryption & Key Management	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection	While CSA CCM mentions general information security controls, it does not define controls for electronic messaging.

9.13 Physical and environmental

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
18 Physical and environmental				
18.1 Asset management				
18.1.2 Level 1 requirements				
18.1.2(a)	INCLUDED	DCS Datacenter Security	DCS 01 - Asset Management	N.A
18.1.2(b)	INCLUDED	DCS Datacenter Security	DCS 01 - Asset Management	N.A
18.1.2(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 03 - Datacenter Utilities / Environmental Conditions	N.A
18.1.2(d)	INCLUDED	N.A	N.A	CSA CCM does not specify controls to disconnect unused hardware devices. Note: ISO/IEC 27001:2013 covers this requirement under Section A.11.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
18.1.2(e)	INCLUDED	HRS Human Resources	HRS 12 - Workspace	CSA CCM mandates that policies and procedures shall be established to require that unattended workspace is not openly visible, however it does not cover all the equipment's. Note: ISO/IEC 27001:2013 covers this requirement under Section A.11.2.
18.1.2(f)	INCLUDED	HRS Human Resources	HRS 12 - Workspace	N.A
18.1.3 Level 2 requirements				
18.1.3(a)	INCLUDED	N.A	N.A	CSA CCM does not define controls pertaining to decommissioning of devices. Note: ISO/IEC 27001:2013 covers this requirement under Section A.11.2.
18.1.3(b)	INCLUDED	DSI Data Security & Information Lifecycle Management	DSI 08 - Secure Disposal	N.A
18.2 Off-site movement				
18.2.2 Level 1 requirements				
18.2.2(a)	INCLUDED	DCS Datacenter Security	DCS 04 - Off-Site Authorization	N.A
18.2.3 Level 2 requirements				
18.2.3(a)	INCLUDED	DCS Datacenter Security	DCS 04 - Off-Site Authorization	N.A
18.3 Physical access				
18.3.2 Level 1 requirements				
18.3.2(a)	INCLUDED	DCS Datacenter Security	DCS 02 - Controlled Access Points	N.A
18.3.2(b)	INCLUDED	DCS Datacenter Security	DCS 02 - Controlled Access Points DCS 07 - Secure Area Authorization	N.A
18.3.2(c)	INCLUDED	DCS Datacenter Security	DCS 08 - Unauthorized Persons Entry	N.A
18.3.2(d)	INCLUDED	DCS Datacenter Security	DCS 09 - User Access	N.A
18.3.2(e)	INCLUDED	DCS Datacenter Security HRS Human Resources	DCS 09 - User Access HRS-04 - Employment Termination	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
18.3.3 Level 2 requirements				
18.3.3(a)	INCREMENTAL	DCS Datacenter Security	DCS 02 - Controlled Access Points DCS 07 - Secure Area Authorization	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				
18.4.2 Level 1 requirements				
18.4.2(a)	INCREMENTAL	DCS Datacenter Security	DCS 07 - Secure Area Authorization DCS 08 - Unauthorized Persons Entry	CSA CCM does not define specific security controls to control and restrict visitor access via the use of escorts.
18.4.2(b)	INCREMENTAL	DCS Datacenter Security	DCS 07 - Secure Area Authorization DCS 08 - Unauthorized Persons Entry	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	DCS Datacenter Security	DCS 07 - Secure Area Authorization DCS 08 - Unauthorized Persons Entry	CSA CCM does not define specific security controls to control and restrict visitor access via logs.
18.4.2(d)	INCREMENTAL	DCS Datacenter Security	DCS 07 - Secure Area Authorization DCS 08 - Unauthorized Persons Entry	CSA CCM does not define specific security controls to control and restrict visitor access logs should be periodically reviewed.
18.4.2(e)	INCLUDED	DCS Datacenter Security	DCS 02 - Controlled Access Points DCS 09 - User Access	N.A
18.4.3 Level 2 requirements				
18.4.3(a)	NEW	N.A	N.A	CSA CCM does not define specific security controls to control and restrict visitor access via obtaining management approval in specific situations.
18.5 Environmental threats and equipment power failures				
18.5.2 Level 1 requirements				
18.5.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience DCS Datacenter Security	BCR 05 - Environmental Risks DCS 06 - Policy	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
18.5.2(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience DCS Datacenter Security	BCR 03 - Datacenter Utilities / Environmental Conditions BCR 05 - Environmental Risks DCS 09 - User Access	N.A
18.5.2(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 03 - Datacenter Utilities / Environmental Conditions	N.A
18.5.2(d)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 05 - Environmental Risks	N.A
18.5.2(e)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 05 - Environmental Risks	N.A
18.5.2(f)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 03 - Datacenter Utilities / Environmental Conditions	N.A
18.5.2(g)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 03 - Datacenter Utilities / Environmental Conditions	While CSA CCM defines controls for environmental security, it does not require protection of power systems from the effects of large amounts of systems being turned on simultaneously. Note: ISO/IEC 27001:2013 covers this requirement under Section A.11.2.
18.5.2(h)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 03 - Datacenter Utilities / Environmental Conditions BCR 08 - Equipment Power Failures	N.A
18.6 Physical security review				
18.6.2 Level 1 requirements				
18.6.2(a)	INCLUDED	AAC Audit Assurance & Compliance DCS Datacenter Security	AAC 02 - Independent Audits DCS 02 - Controlled Access Points	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
18.6.2(b)	INCREMENTAL	AAC Audit Assurance & Compliance	AAC 02 - Independent Audits	CSA CCM defines that reviews need to be performed annually; however, it does not define periodical review of physical security.

9.14 Operations

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
19 Operations				
19.1 Operations management policies and procedures				
19.1.3 Level 2 requirements				
19.1.3(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 04 - Documentation	N.A
19.2 Documentation of service operations and external dependencies				
19.2.2 Level 1 requirements				
19.2.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 04 - Documentation BCR 09 - Impact Analysis	N.A
19.2.4 Level 3 requirements				
19.2.4(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 04 - Documentation BCR 09 - Impact Analysis	N.A
19.3 Capacity management				
19.3.2 Level 1 requirements				
19.3.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 04 - Information System Documentation	N.A
19.3.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 04 - Information System Documentation	N.A
19.3.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
19.3.4(a)	INCLUDED	CCC Change Control & Configuration Management IVS Infrastructure & Virtualization Security	CCC 03 - Quality Testing IVS 04 - Information System Documentation	While monitoring and alerts are mentioned, CSA CCM does not require the implementation of automated monitoring tools to monitor critical resources for capacity utilisation, and alert notification types and rules be appropriately configured. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.1.
19.4 Service levels				
19.4.3 Level 2 requirements				
19.4.3(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
19.4.3(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
19.4.3(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
19.4.4 Level 3 requirements				
19.4.4(a)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	CSA CCM does not explicitly require the communication of redundant network connectivity to cloud users. Note: ISO/IEC 27001:2013 covers this requirement under Sections 4.2, 4.3 and 7.4.
19.4.4(b)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	CSA CCM does not explicitly require the communication of minimum bandwidth available to cloud users. Note: ISO/IEC 27001:2013 covers this requirement under Sections 4.2, 4.3 and 7.4.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
19.4.4(c)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
19.4.4(d)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	CSA CCM does not explicitly require the communication of QoS to cloud users. Note: ISO/IEC 27001:2013 covers this requirement under Sections 4.2, 4.3 and 7.4.
19.4.4(e)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	CSA CCM does not explicitly require the communication of bandwidth scalability on storage links to cloud users. Note: ISO/IEC 27001:2013 covers this requirement under Sections 4.2, 4.3 and 7.4.
19.4.4(f)	INCLUDED	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements	N.A
19.5 Reliability and resiliency				
19.5.4 Level 3 requirements				
19.5.4(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience IVS Infrastructure & Virtualization Security	BCR 09 - Impact Analysis IVS 06 - Network Security	N.A
19.5.4(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	While CSA CCM defines strong technical controls to ensure security, however, it does not require resiliency for storage systems. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.17.1 and A.17.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
19.5.4(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 03 - Datacenter Utilities / Environmental Conditions BCR 08 - Equipment Power Failures	While CSA CCM covers redundancies for equipment in general, it does not cover redundancy for SAN components. Note: ISO/IEC 27001:2013 covers this requirement under Section A.17.2.
19.5.4(d)	INCLUDED	BCR Business Continuity Management & Operational Resilience IVS Infrastructure & Virtualization Security	BCR-12 - Retention Policy IVS 06 - Network Security	While CSA CCM defines controls related to backup and recovery, it does not explicitly state that multiple links and switches should be installed for all I / O operations. Note: ISO/IEC 27001:2013 covers this requirement under Section A.17.2.
19.5.4(e)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	While CSA CCM covers network security in general, it does not specifically require the high availability of network and storage components. Note: ISO/IEC 27001:2013 covers this requirement under Section A.17.2.
19.5.4(f)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis BCR-10 - Management Program	While CSA CCM defines control for business resiliency, it does not explicitly cover implementation of RAID. Note: ISO/IEC 27001:2013 covers this requirement under Section A.17.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
19.5.4(g)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis BCR 10 - Management Program	While CSA CCM defines controls for handling disruption, it does not cover the usage of hot spares to reduce the impact of failures in storage arrays. Note: ISO/IEC 27001:2013 covers this requirement under Section A.17.2.
19.5.4(h)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience IVS Infrastructure & Virtualization Security	BCR 10 - Management Program IVS 01 - Audit Logging / Intrusion Detection	CSA CCM does not require the installation of capabilities for early detection of warnings and outages of storage systems.
19.6 Recoverability				
19.6.3 Level 2 requirements				
19.6.3(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 06 - Equipment Location BCR 07 - Equipment Maintenance BCR 08 - Equipment Power Failures	N.A
19.6.3(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	N.A

9.15 Change management

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
20 Change management				
20.1 Change management process				
20.1.2 Level 1 requirements				
20.1.2(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 05 - Production Changes	N.A
20.1.3 Level 2 requirements				
20.1.3(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 05 - Production Changes	N.A
20.1.3(b)	INCLUDED	CCC Change Control & Configuration Management	CCC 05 - Production Changes	N.A
20.2 Backup procedures				
20.2.2 Level 1 requirements				
20.2.2(a)	INCLUDED	CCC Change Control & Configuration Management	CCC 05 - Production Changes	While CSA CCM defines controls for change management process, it does not explicitly mention about performing backups of the affected systems prior to the implementation of change. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.3.
20.3 Back-out or rollback procedures				
20.3.3 Level 2 requirements				
20.3.3(a)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 05 - Production Changes	While CSA CCM defines controls for change management process, it does not explicitly mention about designing rollback option.
20.3.4 Level 3 requirements				
20.3.4(a)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 05 - Production Changes	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.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
20.4 Separation of environment				
20.4.2 Level 1 requirements				
20.4.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 08 - Production / Non-Production Environments	N.A
20.5 Patch management procedures				
20.5.2 Level 1 requirements				
20.5.2(a)	INCLUDED	TVM Threat and Vulnerability Management	TVM 02 - Vulnerability / Patch Management	N.A
20.5.2(b)	INCREMENTAL	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 02 - Vulnerability / Patch Management	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.
20.5.3 Level 2 requirements				
20.5.3(a)	INCLUDED	TVM Threat and Vulnerability Management	TVM 02 - Vulnerability / Patch Management	N.A
20.5.3(b)	INCLUDED	TVM Threat and Vulnerability Management	TVM 02 - Vulnerability / Patch Management	N.A
20.5.3(c)	INCREMENTAL	TVM Threat and Vulnerability Management	TVM 02 - Vulnerability / Patch Management	While CSA CCM defines that patches should be implemented, it does not specify controls to test the patches.
20.5.3(d)	INCREMENTAL	IVS Infrastructure & Virtualization Security TVM Threat and Vulnerability Management	IVS 07 - OS Hardening and Base Controls TVM 02 - Vulnerability / Patch Management	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.
20.5.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
20.5.4(a)	INCREMENTAL	TVM Threat and Vulnerability Management	TVM 02 - Vulnerability / Patch Management	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.

9.16 Business continuity planning (BCP) and disaster recovery (DR)

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
21 Business continuity planning (BCP) and disaster recovery (DR)				
21.1 BCP framework				
21.1.2 Level 1 requirements				
21.1.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 09 - Impact Analysis BCR 10 - Management Program	N.A
21.1.2(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 09 - Impact Analysis BCR 10 - Management Program	N.A
21.1.2(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 09 - Impact Analysis BCR-10 - Management Program	N.A
21.1.2(d)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis	N.A
21.1.2(e)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
21.1.2(f)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 09 - Impact Analysis BCR-10 - Management Program BCR-12 - Retention Policy	N.A
21.1.3 Level 2 requirements				
21.1.3(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis	N.A
21.1.3(b)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis	Recovery Point Objective (RPO) is not explicitly mentioned in CSA CCM.
21.2 BCP and DR plans				
21.2.2 Level 1 requirements				
21.2.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis	N.A
21.2.2(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 10 - Management Program	N.A
21.2.2(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 04 - Documentation BCR 10 - Management Program	N.A
21.2.2(d)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 06 - Equipment Location	N.A
21.2.4 Level 3 requirements				
21.2.4(a)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	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.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
21.2.4(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 09 - Impact Analysis	N.A
21.2.4(c)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 09 - Impact Analysis	Recovery Point Objective (RPO) is not explicitly mentioned in CSA CCM.
21.2.4(d)	INCLUDED	BCR Business Continuity Management & Operational Resilience DCS Datacenter Security	BCR 06 - Equipment Location DCS 01 - Asset Management DCS 05 - Off-Site Equipment	N.A
21.3 BCP and DR testing				
21.3.2 Level 1 requirements				
21.3.2(a)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 02 - Business Continuity Testing	N.A
21.3.4 Level 3 requirements				
21.3.4(a)	INCREMENTAL	BCR Business Continuity Management & Operational Resilience	BCR 01 - Business Continuity Planning BCR 02 - Business Continuity Testing	CSA CCM requires business continuity plans to be tested at planned intervals but does not specify the frequency of such tests.
21.3.4(b)	INCLUDED	BCR Business Continuity Management & Operational Resilience	BCR 12 - Retention Policy	N.A
21.3.4(c)	INCLUDED	BCR Business Continuity Management & Operational Resilience EKM Encryption & Key Management GRM Governance and Risk Management	BCR 12 - Retention Policy EKM 03 - Sensitive Data Protection GRM 02 - Data Focus Risk Assessments	N.A

9.17 Cloud services administration

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22 Cloud services administration				
22.1 Privilege account creation				
22.1.2 Level 1 requirements				
22.1.2(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	N.A
22.1.2(b)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	N.A
22.1.2(c)	INCLUDED	IAM Identity & Access Management	IAM 09 - User Access Authorization	N.A
22.1.2(d)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 05 - Segregation of Duties	While CSA CCM covers user accounts in general, it does not specifically require that privileged accounts shall not be used as system or service accounts. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.2.
22.2 Generation of administrator passwords				
22.2.2 Level 1 requirements				
22.2.2(a)	INCLUDED	MOS Mobile Security	MOS 16 - Passwords	While CSA CCM requires password policies to be documented and enforced, specific details of such password policies are not mentioned. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.4.

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.2.2(b)	INCLUDED	MOS Mobile Security	MOS 16 - Passwords	While CSA CCM requires password policies to be documented and enforced, it does not specifically require that general passwords should be disallowed. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.4.
22.2.2(c)	INCREMENTAL	MOS Mobile Security	MOS 16 - Passwords	While CSA CCM requires password policies to be documented and enforced, it does not specifically require that shared passwords with other accounts be disallowed.
22.2.3 Level 2 requirements				
22.2.3(a)	INCREMENTAL	MOS Mobile Security	MOS 16 - Passwords	While CSA CCM requires password policies to be documented and enforced, specific details of such password policies are not mentioned.
22.2.3(b)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	N.A
22.2.3(c)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	N.A
22.3 Administrator access review and revocation				
22.3.2 Level 1 requirements				
22.3.2(a)	INCLUDED	IAM Identity & Access Management	IAM 11 - User Access Revocation	N.A
22.3.2(b)	INCLUDED	IAM Identity & Access Management	IAM 10 - User Access Reviews	N.A
22.3.2(c)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 11 - User Access Revocation IAM 12 - User ID Credentials	While CSA CCM defines account management controls, it does not require removal of inactive accounts every 90 days.

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.3.2(d)	INCLUDED	IAM Identity & Access Management	IAM 11 - User Access Revocation	N.A
22.3.3 Level 2 requirements				
22.3.3(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 04 - Policies and Procedures	N.A
22.4 Account lockout				
22.4.2 Level 1 requirements				
22.4.2(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines user access controls, it does not specifically allow a maximum of six (6) unsuccessful attempts.
22.4.2(b)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines user access controls, it does not specify lockout duration.
22.4.3 Level 2 requirements				
22.4.3(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines user access controls, it does not specifically require that only an administrator can manually unlock the account.
22.5 Password change				
22.5.2 Level 1 requirements				
22.5.2(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM requires password policies to be documented and enforced, it does not specifically require the enforcement of compulsory password change based on industry standard practices. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.4.

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.5.2(b)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	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.
22.5.3 Level 2 requirements				
22.5.3(a)	INCLUDED	EKM Encryption & Key Management IAM Identity & Access Management	EKM 02 - Key Generation IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	N.A
22.6 Password reset and first logon				
22.6.2 Level 1 requirements				
22.6.2(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	CSA CCM does not specifically require the generation of unique passwords and mandating of password change upon first login.
22.6.2(b)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	CSA CCM does not specifically require the verification of identity prior to changing password.
22.6.2(c)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	CSA CCM does not specifically require management approval to be obtained in the event of a password reset.
22.6.2(d)	INCREMENTAL	IAM Identity & Access Management MOS Mobile Security	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials MOS 16 - Passwords	CSA CCM does not specifically require the reset of password in the event of the second factor device being lost.
22.6.3 Level 2 requirements				
22.6.3(a)	INCREMENTAL	IAM Identity & Access Management MOS Mobile Security	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials MOS 16 - Passwords	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.
22.6.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.6.4(a)	INCREMENTAL	IAM Identity & Access Management MOS Mobile Security	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials MOS 16 - Passwords	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				
22.7.2 Level 1 requirements				
22.7.2(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	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(b)	INCLUDED	DCS Datacenter Security	DCS 03 - Equipment Identification	N.A
22.7.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	While CSA CCM defines control for access management, it does not limit the control of local administrative accounts. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.2.
22.7.2(d)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While policies and procedures on user access are mentioned, CSA CCM does not require that explicit approval be obtained if local administrative access is enabled or required. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.2.
22.7.2(e)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	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.
22.7.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.7.3(a)	NEW	N.A	N.A	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.
22.7.4 Level 3 requirements				
22.7.4(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	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.
22.8 Administrator access logs				
22.8.2 Level 1 requirements				
22.8.2(a)	INCLUDED	IAM Identity & Access Management	IAM 10 - User Access Reviews	While CSA CCM covers access review in general, it does not specifically require an establishment of a procedure to review administrator activities periodically. Note: ISO/IEC 27001:2013 covers this requirement under Sections 5.2 and A.9.2.
22.8.3 Level 2 requirements				
22.8.3(a)	INCLUDED	GRM Governance and Risk Management IAM Identity & Access Management IVS Infrastructure & Virtualization Security	GRM 07 - Policy Enforcement IAM 10 - User Access Reviews IVS 01 - Audit Logging / Intrusion Detection	N.A
22.8.4 Level 3 requirements				
22.8.4(a)	INCLUDED	IAM Identity & Access Management	IAM 04 - Policies and Procedures	N.A
22.9 Session management				

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.9.2 Level 1 requirements				
22.9.2(a)	INCLUDED	HRS Human Resources IAM Identity & Access Management	HRS 12 - Workspace IAM 02 - Credential Lifecycle / Provision Management	N.A
22.9.2(a)	INCREMENTAL	HRS Human Resources IAM Identity & Access Management	HRS 12 - Workspace IAM 02 - Credential Lifecycle / Provision Management	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 exceeds 15 minutes.
22.10 Segregation of duties				
22.10.2 Level 1 requirements				
22.10.2(a)	INCREMENTAL	IAM Identity & Access Management	IAM 05 - Segregation of Duties IAM 10 - User Access Reviews	While CSA CCM covers access rights review and segregation of duties, it does not specifically such review to be conducted annually.
22.10.2(b)	INCLUDED	DSI Data Security & Information Lifecycle Management IVS Infrastructure & Virtualization Security IAM Identity & Access Management	DSI 06 - Non-Production Data IVS 08 - Production / Non-Production Environments IAM 05 - Segregation of Duties	N.A
22.10.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security IAM Identity & Access Management	IVS 08 - Production / Non-Production Environments IAM 05 - Segregation of Duties	While CSA CCM covers the separation of the production and non-production environments to prevent unauthorised access, it does not cover the restriction of access to backups. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.6.1 and A.9.2.
22.10.3 Level 2 requirements				
22.10.3(a)	INCREMENTAL	IAM Identity & Access Management	IAM 05 - Segregation of Duties IAM 10 - User Access Reviews	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.

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.10.4 Level 3 requirements				
22.10.4(a)	INCREMENTAL	IAM Identity & Access Management	IAM 05 - Segregation of Duties IAM 10 - User Access Reviews	While CSA CCM covers access rights review and segregation of duties, it does not specifically such review to be conducted on a monthly basis.
22.11 Secure transmission of access credentials				
22.11.2 Level 1 requirements				
22.11.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	N.A
22.12 Third party administrative access				
22.12.2 Level 1 requirements				
22.12.2(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 05 - Segregation of Duties IAM 07 - Third Party Access	N.A
22.12.2(b)	INCLUDED	IAM Identity & Access Management	IAM 07 - Third Party Access	While CSA CCM defines controls to perform risk assessment on third party access, it does not explicitly state that vendor access should be monitored. Note: ISO/IEC 27001:2013 covers this requirement under Section A.15.2.
22.12.3 Level 2 requirements				
22.12.3(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 11 - User Access Revocation IAM 12 - User ID Credentials IAM 07 - Third Party Access	While CSA CCM defines controls to perform risk assessment on third party access, it does not explicitly require monitoring and termination after the usage of remote access given to third parties. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.9.2 and A.15.1.
22.12.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.12.4(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	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				
22.13.2 Level 1 requirements				
22.13.2(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines controls for user access policies and procedures, it does not explicitly cover service and application accounts.
22.13.3 Level 2 requirements				
22.13.3(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines controls for user access policies and procedures, it does not cover service and application accounts.
22.13.3(b)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	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	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	While CSA CCM requires all the Operating System to be hardened, it does not explicitly cover restricting simultaneous logins.
22.13.3(d)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	N.A
22.13.3(e)	INCREMENTAL	AIS Application & Interface Security	AIS 01 - Application Security	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.
22.13.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CCM clauses	Reference to matching CCM sub-clauses	Remarks on identified gaps
22.13.4(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM defines controls for user access policies and procedures, it does not cover the change of service account passwords.

9.18 Cloud user access

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
23 Cloud user access				
23.1 User access registration				
23.1.2 Level 1 requirements				
23.1.2(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM has defined controls for user access management, it does not explicitly state that generic usernames should be disallowed. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.9.2 and A.9.4.
23.1.2(b)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 06 - Source Code Access Restriction	N.A
23.2 User access security				
23.2.2 Level 1 requirements				
23.2.2(a)	INCLUDED	IAM Identity & Access Management	IAM 09 - User Access Authorization	While CSA CCM defines controls to obtain approval for granting access, it does not state that it should be documented. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
23.2.2(b)	INCLUDED	IAM Identity & Access Management IVS Infrastructure & Virtualization Security	IAM 04 - Policies and Procedures IVS 01 - Audit Logging / Intrusion Detection	N.A
23.2.2(c)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM has defined controls for user access management, CSA CCM does not mandate to implement a default deny-all setting.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
23.2.2(d)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	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	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	While CSA CCM states that traffic should be restricted and monitored, it does not explicitly specify anti-bot controls to be implemented.
23.2.3 Level 2 requirements				
23.2.3(a)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	CSA CCM specifies implementation of multi-factor authentication.
23.2.4 Level 3 requirements				
23.2.4(a)	NEW	N.A	N.A	CSA CCM does not explicitly state utilisation of identity management to coordinate and restrict storage of same user identity in multiple cloud environments.
23.3 User access password				
23.3.2 Level 1 requirements				
23.3.2(a)	INCLUDED	MOS Mobile Security IVS Infrastructure & Virtualization Security	MOS 16 Mobile Security - Passwords IVS 12 - Wireless Security	While CSA CCM defines password controls for mobile devices and wireless, it does not define the same requirement for all the other devices / access methods. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.4.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
23.3.2(b)	INCLUDED	MOS Mobile Security IVS Infrastructure & Virtualization Security	MOS 16 Mobile Security - Passwords IVS 12 - Wireless Security	While CSA CCM defines password controls for mobile devices and wireless, CSA CCM does not explicitly prohibit use of generic passwords for other devices / access methods. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.4.
23.3.2(c)	INCREMENTAL	MOS Mobile Security IVS Infrastructure & Virtualization Security	MOS 16 - Passwords IVS 12 - Wireless Security	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.
23.3.3 Level 2 requirements				
23.3.3(a)	INCREMENTAL	MOS Mobile Security IVS Infrastructure & Virtualization Security	MOS 16 - Passwords IVS 12 - Wireless 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				
23.4.2 Level 1 requirements				
23.4.2(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.4.2(b)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.4.3 Level 2 requirements				
23.4.3(a)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.4.3(b)	INCREMENTAL	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM mandates user access policies, it does not specify user ID lockout parameters.
23.5 User password reset and 1st logon change				
23.5.2 Level 1 requirements				
23.5.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 12 - Wireless Security	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
23.5.2(b)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	CSA CCM does not specify password controls related to first time logon.
23.6 Password protection				
23.6.2 Level 1 requirements				
23.6.2(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.6.2(b)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.6.2(c)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.7 User session management				
23.7.2 Level 1 requirements				
23.7.2(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define session controls.
23.7.2(b)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.7.2(c)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define session controls.
23.7.3 Level 2 requirements				
23.7.3(a)	INCLUDED	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not explicitly define controls related to remote access. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.9.2 and A.15.2.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
23.7.4 Level 3 requirements				
23.7.4(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define connection time restrictions for applications.
23.8 Change of cloud user's administrator details notification				
23.8.3 Level 2 requirements				
23.8.3(a)	INCREMENTAL	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements AIS 02 - Customer Access Requirements	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	STA Supply Chain Management, Transparency and Accountability	STA 05 - Supply Chain Agreements AIS 02 - Customer Access Requirements	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.
23.9 Self-service portal creation and management of user accounts				
23.9.2 Level 1 requirements				
23.9.2(a)	INCREMENTAL	GRM Governance and Risk Management	GRM 04 - Management Program	While CSA CCM defines controls pertaining to access control, it does not define password parameters.
23.9.2(b)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management	N.A
23.9.3 Level 2 requirements				
23.9.3(a)	INCLUDED	IAM Identity & Access Management	IAM 09 - User Access Authorization	N.A
23.10 Communication with cloud users				
23.10.2 Level 1 requirements				
23.10.2(a)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 05 - Production Changes	While CSA CCM mentions notification to cloud users, it does not specify that a procedure should be designed for distributing notifications.
23.10.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
23.10.3(a)	INCREMENTAL	HRS Human Resources	HRS 10 - Training / Awareness	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.

9.19 Tenancy and customer isolation

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24 Tenancy and customer isolation				
24.1 Multi tenancy				
24.1.2 Level 1 requirements				
24.1.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security IVS 08 - Production / Non-Production Environments IVS 09 - Segmentation	N.A
24.1.2(b)	INCLUDED	DSI Data Security & Information Lifecycle Management IVS Infrastructure & Virtualization Security	DSI 02 - Data Inventory / Flows IVS 09 - Segmentation	N.A
24.1.2(c)	INCLUDED	AIS Application & Interface Security DSI Data Security & Information Lifecycle Management IVS Infrastructure & Virtualization Security	AIS 04 - Data Security / Integrity DSI 02 - Data Inventory / Flows IVS 09 - Segmentation	N.A
24.1.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.1.4(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 01 - Audit Logging / Intrusion Detection IVS 06 - Network Security	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.
24.1.4(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 09 - Segmentation	N.A
24.1.4(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	N.A
24.2.3 Level 2 requirements				
24.2.3(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	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	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security IVS 09 - Segmentation	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	IVS Infrastructure & Virtualization Security IAM Identity & Access Management	IVS 09 - Segmentation IAM 02 - Credential Lifecycle / Provision Management	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.
24.2.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.2.4(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 09 - Segmentation IVS 06 - Network Security	N.A
24.3				
24.3.2 Level 1 requirements				
24.3.2(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 05 - Vulnerability Management IVS 06 - Network Security IVS 09 - Segmentation	N.A
24.3.2(b)	INCLUDED	IVS Infrastructure & Virtualization Security EKM Encryption & Key Management IVS Infrastructure & Virtualization Security	AIS 04 - Data Security / Integrity EKM 03 - Sensitive Data Protection IVS 06 - Network Security IVS 09 - Segmentation	N.A
24.3.2(c)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	N.A
24.3.2(d)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security IVS 09 - Segmentation	While CSA CCM requires the network infrastructure to be compliant with relevant legal, statutory, and regulatory requirements, it does not specifically require that the network infrastructure and configurations be compared against with industry standards. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
24.3.2(e)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	N.A
24.3.2(f)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.3.2(g)	INCLUDED	IAM Identity & Access Management IVS Infrastructure & Virtualization Security	IAM 02 - Credential Lifecycle / Provision Management IAM 04 - Policies and Procedures IVS 11 - VMM Security - Hypervisor Hardening	N.A
24.3.2(h)	INCLUDED		IAM 07 - Third Party Access IVS 06 - Network Security	N.A
24.3.2(i)	INCLUDED	DSI Data Security & Information Lifecycle Management IVS Infrastructure & Virtualization Security	DSI 02 - Data Inventory / Flows IVS 06 - Network Security	N.A
24.3.2(j)	INCLUDED	IAM Identity & Access Management	IAM 02 - Credential Lifecycle / Provision Management IAM 12 - User ID Credentials	N.A
24.3.2(k)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 -Network Security IVS 09 - Segmentation IVS 11 - VMM Security - Hypervisor Hardening	N.A
24.3.2(l)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 11 - VMM Security - Hypervisor Hardening	N.A
24.3.2(m)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security IVS 12 - Wireless Security	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.
24.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.3.3(a)	INCLUDED	EKM Encryption & Key Management IVS Infrastructure & Virtualization Security	EKM 03 - Sensitive Data Protection IVS 06 - Network Security	N.A
24.3.3(b)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	N.A
24.3.3(c)	INCREMENTAL	EKM Encryption & Key Management	EKM 03 - Sensitive Data Protection	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	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	While CSA CCM defines controls to secure network environment, it does not explicitly cover stateful inspection.
24.3.3(e)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security	While CSA CCM defines controls to secure network environment, it does not cover the disclosure of internal IP addresses.
24.3.3(f)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 06 - Network Security IVS 09 - Segmentation IVS 12 - Wireless Security	N.A
24.3.4 Level 3 requirements				
24.3.4(a)	INCLUDED	IVS Infrastructure & Virtualization Security	IVS 09 - Segmentation	N.A
24.4 Virtualisation				
24.4.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.4.2(a)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 04 - Information System Documentation IVS 05 - Management - Vulnerability Management IVS 06 - Network Security IVS 07 - OS Hardening and Base Controls IVS 09 - Segmentation IVS 10 - vMotion Data Protection IVS 11 - VMM Security - Hypervisor Hardening	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(b)	INCLUDED	GRM Governance and Risk Management	GRM 02 - Data Focus Risk Assessments GRM 08 - Policy Impact on Risk Assessments GRM 10 - Risk Assessments	N.A
24.4.2(c)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 02 Infrastructure & Virtualization Security - Change Detection IVS 11 - VMM Security - Hypervisor Hardening	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 Level 1 requirements				
24.5.2(a)	INCREMENTAL	AIS Application & Interface Security IAM Identity & Access Management	AIS 02 - Customer Access Requirements AIS 04 - Data Security / Integrity IAM 02 - Credential Lifecycle / Provision Management	While CSA CCM covers access control requirements in general, it does not specifically cover access to network attached storage devices.

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.5.2(b)	INCREMENTAL	CCC Change Control & Configuration Management	CCC 05 - Production Changes	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.
24.5.3 Level 2 requirements				
24.5.3(a)	INCLUDED	IVS Infrastructure & Virtualization Security IAM Identity & Access Management	IAM 08 - Trusted Sources IVS 06 - Network Security	N.A
24.5.3(b)	INCLUDED	IAM Identity & Access Management	IAM 03 - Diagnostic / Configuration Ports Access	N.A
24.5.3(c)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 07 - OS Hardening and Base Controls	While CSA CCM defines hardening of operating system, it does not cover mutual authentication between devices.
24.5.3(d)	NEW	N.A	N.A	CSA CCM does not require that storage devices shall only respond to requests from authorised devices.
24.5.3(e)	NEW	N.A	N.A	CSA CCM does not cover automatic replication.
24.5.4 Level 3 requirements				
24.5.4(a)	NEW	N.A	N.A	CSA CCM does not cover hard zones.
24.5.4(b)	NEW	N.A	N.A	CSA CCM does not cover Logical Unit Numbers (LUN).
24.5.4(c)	INCLUDED	EKM Encryption & Key Management	EKM 03 - Sensitive Data Protection	N.A

MTCS clause	Gaps	Reference to matching CSA CCM clauses	Reference to matching CSA CCM sub-clauses	Remarks on identified gaps
24.5.4(d)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation EKM 04 - Storage and Access	N.A
24.6 Data segregation				
24.6.3 Level 2 requirements				
24.6.3(a)	INCREMENTAL	EKM Encryption & Key Management	EKM 02 - Key Generation	While CSA CCM covers segregation for encryption keys, segregation for data access and logs are not mentioned.
24.6.3(b)	INCREMENTAL	DCS Datacenter Security	DCS 04 - Off-Site Authorization	While CSA CCM covers authorisation controls, it does not cover segregation controls for offsite data storage and recovery.
24.6.4 Level 3 requirements				
24.6.4(a)	INCLUDED	EKM Encryption & Key Management	EKM 02 - Key Generation EKM 04 - Storage and Access	N.A
24.6.4(b)	INCREMENTAL	IVS Infrastructure & Virtualization Security	IVS 09 - Segmentation	While CSA CCM states controls to segment user access, it does not explicitly cover the segregation of backups by cloud users.

<End of Gap Analysis Report>