INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS)
Gap Analysis Report

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

December 2014

Revision History

Revision Date	Version	Updated by	Description
December 2014	Ver. 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 MTCS SS to CSA STAR 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 MTCS SS certified to adopt CSA STAR based on CCM v3.0 and ISO/IEC 27001:2013. 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 the CSA STAR. The information provided in this document aims to assist entities that are MTCS SS certified to adopt the CSA STAR. Cloud Service Providers that are MTCS SS certified will have to comply with the requirements stated in CSA STAR that are not fully covered in MTCS SS.	The purpose of the Implementation Guideline Report is to assist Cloud Service Providers that are MTCS SS certified to implement CSA STAR. 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, CSA STAR certification bodies and external audit bodies in understanding additional requirements beyond MTCS SS. From the Cloud Service Providers' perspective, this document serves as a general guide for them to understand the scope covered in CSA STAR certification audit when the scope of MTCS SS audit overlaps with scope of the CSA STAR.

3 Intended Audience

This Gap Analysis Report is intended for Cloud Service Providers that are MTCS SS certified and interested in obtaining CSA STAR certification for the following scenarios:

Cloud Service Providers that are ISO/IEC 27001:2013 certified

As CSA STAR certification is based upon achieving ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, this report assumes that Cloud Service Providers that are MTCS SS certified are also ISO/IEC 27001:2013 certified (Please refer to https://cloudsecurityalliance.org/star/certification/ for details on CSA STAR certification requirement).

Cloud Service Providers that are not ISO/IEC 27001:2013 certified

This report also caters for Cloud Service Providers that are not ISO/IEC 27001:2013 certified but are interested in obtaining CSA STAR certification. Cloud Service Providers that fall under this category can follow a 2-step approach, as listed below, to obtain CSA STAR certification.

Step 1: Refer to the Gap Analysis Report for cross-certification from MTCS SS to ISO/IEC 27001:2013.
Step 2: Refer to the gaps identified in this report.

The total gaps derived from the 2-step approach above will enable Cloud Service Providers that are not ISO/IEC 27001:2013 certified to obtain CSA STAR certification.

Other than the Cloud Service Providers, this report is also intended to guide auditors, including internal audit function, CSA STAR certification bodies and external audit bodies on the control 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

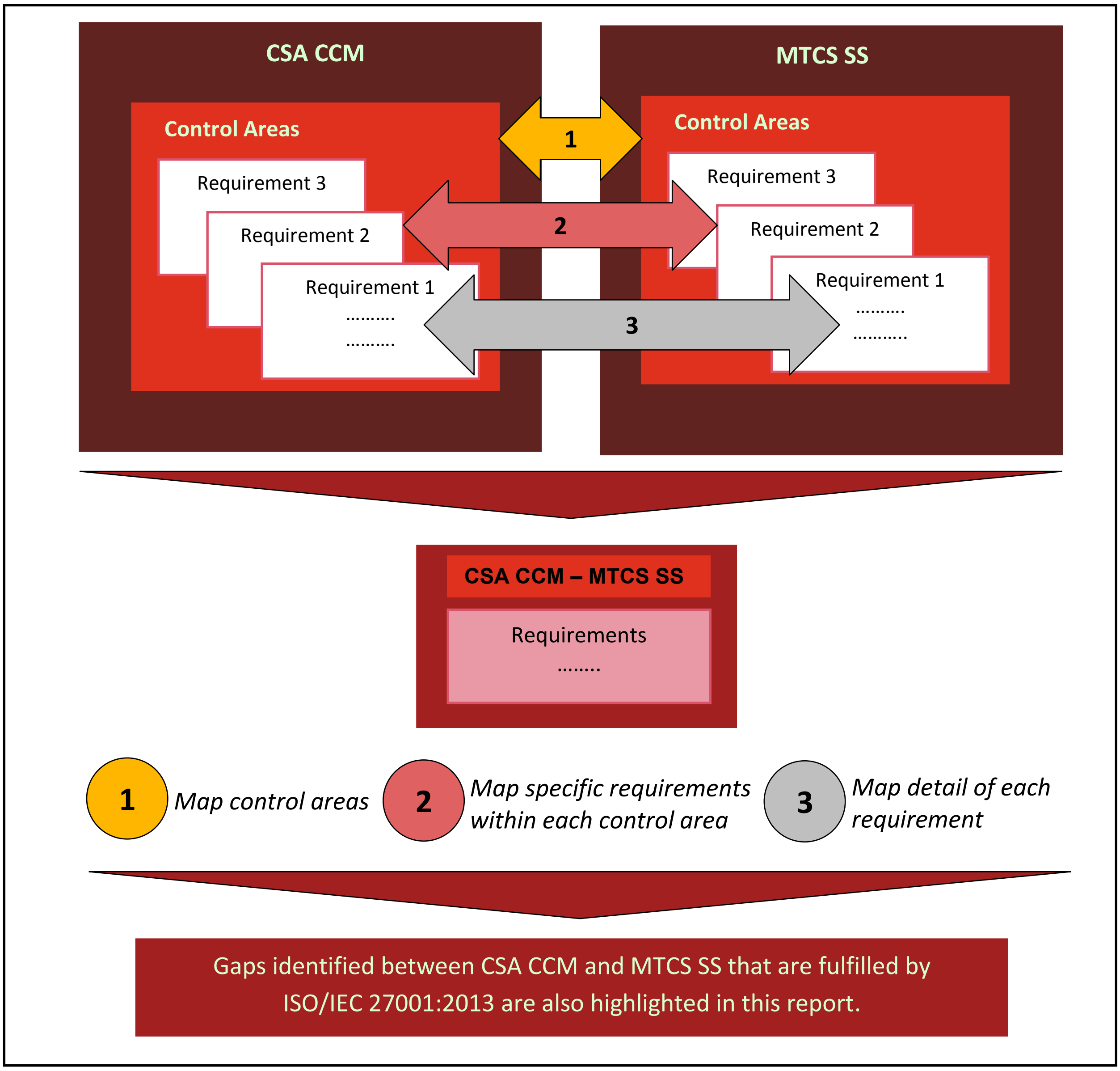
In order to assist entities that are MTCS SS certified to adopt CSA STAR, requirements listed in the MTCS SS were matched with equivalent requirements in CSA CCM. This followed a structured and systematic three (3) step approach:

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

As 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.

*Note: Cloud Service Providers that are not ISO/IEC 27001:2013 certified but are interested in obtaining CSA STAR certification should follow the 2-step approach as described in Section 3 'Intended Audience':

(1) Refer to the Gap Analysis Report for cross-certification from MTCS SS to ISO/IEC 27001:2013; and
(2) Refer to the gaps identified in this report.



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:

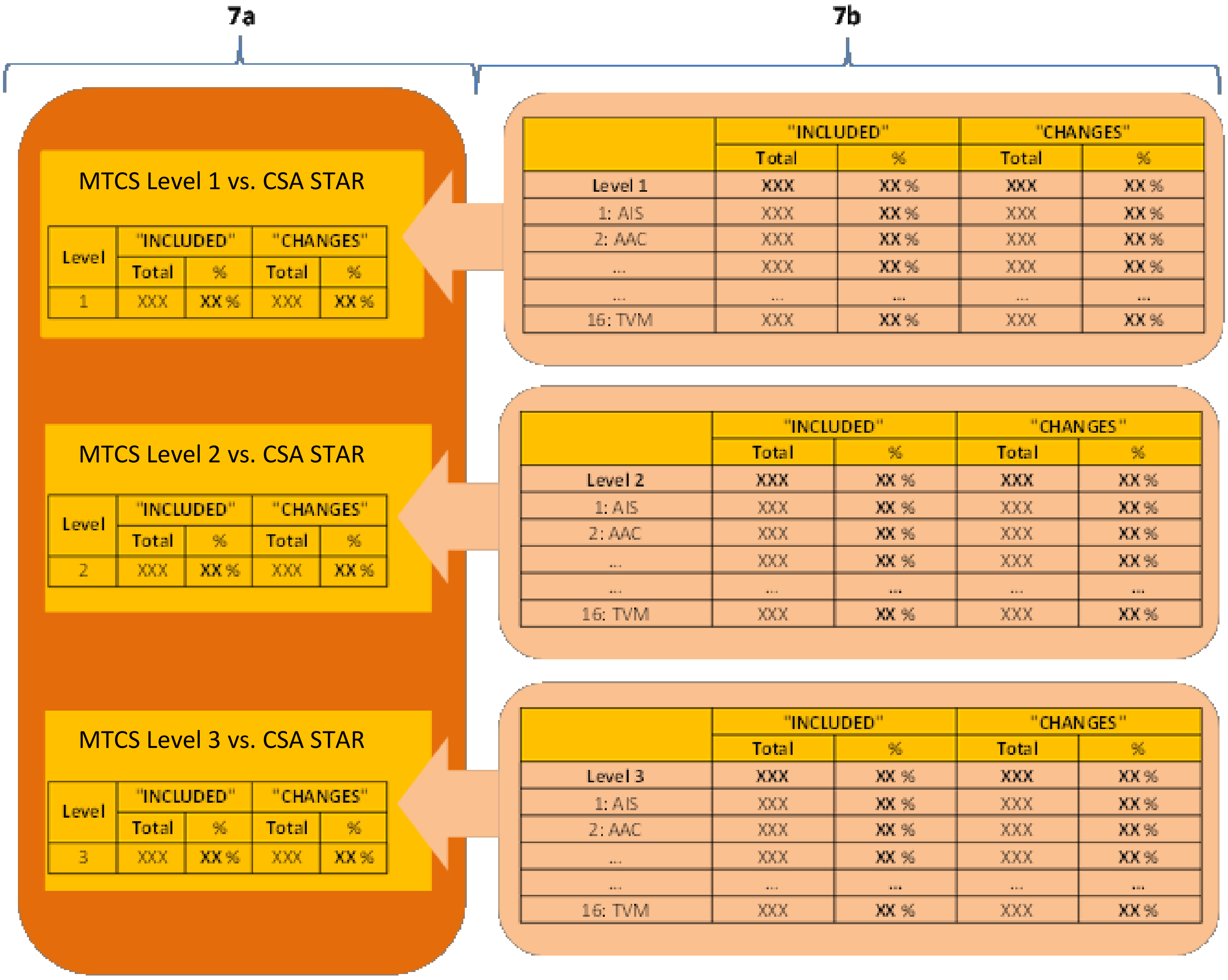
a. Summary by Level in MTCS SS certification (Levels 1, 2 and 3)

Section 7.1 summarises the total gaps identified for each of the three (3) levels of MTCS SS as compared to CSA CCM. As CSA 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 the three (3) levels in MTCS SS as compared to each of the sixteen (16) areas for CSA CCM. 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:



MTCS Level 1 vs. CSA STAR

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

MTCS Level 2 vs. CSA STAR

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

MTCS Level 3 vs. CSA STAR

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

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 1	XXX	XX %	XXX	XX %
1: AIS	XXX	XX %	XXX	XX %
2: AAC	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
16: TVM	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 2	XXX	XX %	XXX	XX %
1: AIS	XXX	XX %	XXX	XX %
2: AAC	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
16: TVM	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 3	XXX	XX %	XXX	XX %
1: AIS	XXX	XX %	XXX	XX %
2: AAC	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
16: TVM	XXX	XX %	XXX	XX %

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

Column	Column description
Total Clauses	Indicates the number of clauses that are currently listed in CSA CCM.
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 statements.
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 MTCS SS characteristics are not costly or onerous in nature.
NEW	Indicates the number of clauses in CSA STAR[1] that are absent, or stated with significantly more detail than the corresponding sections and clauses in MTCS SS. In general, the requirements are classified as "NEW" if there may be material financial cost to meet relevant CSA STAR[1] 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% CSA STAR[1] controls included in MTCS SS.
- Yellow denotes >= 20% and < 50% CSA STAR[1] controls included in MTCS SS.
- Red denotes < 20% CSA STAR[1] controls included in MTCS SS.

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

7.1 Summary by Level in MTCS SS

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

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

Total Controls in CSA CCM	**"INCLUDED"**		**"CHANGES" = "INCREMENTAL" + "NEW"**		**"INCREMENTAL"**		**"NEW"**		**Common Gap(s)[2]**
	Total	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	
136	122	**90%**	14	**10%**	9	**7%**	5	**4%**	2

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

[2] As CSA STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

The table below provides a high level summary of the differences between CSA STAR and MTCS SS Level 2. Cloud Service Providers that are MTCS SS Level 2 certified and looking to be cross certified to CSA STAR can refer to this table for total requirements applicable to this level[1]:

Total Controls in CSA CCM	**"INCLUDED"**		**"CHANGES" = "INCREMENTAL" + "NEW"**		**"INCREMENTAL"**		**"NEW"**		**Common Gaps(s)[2]**
	Total	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	
136	124	**91%**	12	**9%**	7	**5%**	5	**4%**	1

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

[2] As CSA STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

The table below provides a high level summary of the differences between CSA STAR and MTCS SS Level 3. Cloud Service Providers that are MTCS SS Level 3 certified and looking to be cross certified to CSA STAR can refer to this table for total requirements applicable to this level[1]:

Total Controls in CSA CCM	**"INCLUDED"**		**"CHANGES” = “INCREMENTAL” + “NEW”**		**"INCREMENTAL"**		**"NEW"**		**Common Gap(s)[2]**
	Total	**%**	**Total**	**%**	**Total**	**%**	**Total**	**%**	
136	124	**91%**	12	**9%**	7	**5%**	5	**4%**	1

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

[2] As CSA STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

Note that the figures presented in the abovementioned tables fully represent the number of gaps in the respective MTCS SS levels. For example, Cloud Service Providers / auditors only need to refer to MTCS SS Level 3 table for all gaps pertaining to this level if the Cloud Service Provider is already MTCS SS Level 3 certified.

7.2 Summary by Control Area

The purpose of this section is to provide an overview of the differences between MTCS SS and CSA STAR by Control Areas 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 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 STAR[1]:

Section	Topic	Total Clauses in CSA CCM	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"		Common Gap(s)[2]
			Total	%	Total	%	Total	%	Total	%	
1	Application & Interface Security	4	3	**75%**	1	**25%**	1	**25%**	0	**0%**	1
2	Audit Assurance & Compliance	3	3	**100%**	0	**0%**	0	**0%**	0	**0%**	0
3	Business Continuity Management & Operational Resilience	12	12	**100%**	0	**0%**	0	**0%**	0	**0%**	0
4	Change Control & Configuration Management	5	5	**100%**	0	**0%**	0	**0%**	0	**0%**	0
5	Data Security & Information Lifecycle Management	8	7	**88%**	1	**13%**	1	**13%**	0	**0%**	1
6	Datacenter Security	9	9	**100%**	0	**0%**	0	**0%**	0	**0%**	0
7	Encryption & Key Management	4	4	**100%**	0	**0%**	0	**0%**	0	**0%**	0
8	Governance and Risk Management	12	11	**92%**	1	**8%**	1	**8%**	0	**0%**	0
9	Human Resources	12	12	**100%**	0	**0%**	0	**0%**	0	**0%**	0
10	Identity & Access Management	13	13	**100%**	0	**0%**	0	**0%**	0	**0%**	0
11	Infrastructure & Virtualization Security	12	9	**75%**	3	**25%**	3	**25%**	0	**0%**	0
12	Interoperability & Portability	5	2	**40%**	3	**60%**	1	**20%**	2	**40%**	0
13	Mobile Security	20	15	**75%**	5	**25%**	2	**10%**	3	**15%**	0
14	Security Incident Management, E-Discovery & Cloud Forensics	5	5	**100%**	0	**0%**	0	**0%**	0	**0%**	0
15	Supply Chain Management, Transparency and Accountability	9	9	**100%**	0	**0%**	0	**0%**	0	**0%**	0
16	Threat and Vulnerability Management	3	3	**100%**	0	**0%**	0	**0%**	0	**0%**	0
	TOTAL	**136**	**122**	**90%**	**14**	**10%**	**9**	**7%**	**5**	**4%**	**2**

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

[2] As CSA STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

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

Section	Topic	Total Clauses in CSA CCM	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"		Common Gap(s)[2]
			Total	%	Total	%	Total	%	Total	%	
1	Application & Interface Security	4	3	75%	1	25%	1	25%	0	0%	1
2	Audit Assurance & Compliance	3	3	100%	0	0%	0	0%	0	0%	0
3	Business Continuity Management & Operational Resilience	12	12	100%	0	0%	0	0%	0	0%	0
4	Change Control & Configuration Management	5	5	100%	0	0%	0	0%	0	0%	0
5	Data Security & Information Lifecycle Management	8	8	100%	0	0%	0	0%	0	0%	0
6	Datacenter Security	9	9	100%	0	0%	0	0%	0	0%	0
7	Encryption & Key Management	4	4	100%	0	0%	0	0%	0	0%	0
8	Governance and Risk Management	12	12	100%	0	0%	0	0%	0	0%	0
9	Human Resources	12	12	100%	0	0%	0	0%	0	0%	0
10	Identity & Access Management	13	13	100%	0	0%	0	0%	0	0%	0
11	Infrastructure & Virtualization Security	12	9	75%	3	25%	3	25%	0	0%	0
12	Interoperability & Portability	5	2	40%	3	60%	1	20%	2	40%	0
13	Mobile Security	20	15	75%	5	25%	2	10%	3	15%	0
14	Security Incident Management, E-Discovery & Cloud Forensics	5	5	100%	0	0%	0	0%	0	0%	0
15	Supply Chain Management, Transparency and Accountability	9	9	100%	0	0%	0	0%	0	0%	0
16	Threat and Vulnerability Management	3	3	100%	0	0%	0	0%	0	0%	0
	TOTAL	**136**	**124**	**91%**	**12**	**9%**	**7**	**5%**	**5**	**4%**	**1**

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

[2] As CSA STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

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

Section	Topic	Total Clauses in CSA CCM	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"		Common Gap(s)[2]
			Total	%	Total	%	Total	%	Total	%	
1	Application & Interface Security	4	3	**75%**	1	**25%**	1	**25%**	0	**0%**	1
2	Audit Assurance & Compliance	3	3	**100%**	0	**0%**	0	**0%**	0	**0%**	0
3	Business Continuity Management & Operational Resilience	12	12	**100%**	0	**0%**	0	**0%**	0	**0%**	0
4	Change Control & Configuration Management	5	5	**100%**	0	**0%**	0	**0%**	0	**0%**	0
5	Data Security & Information Lifecycle Management	8	8	**100%**	0	**0%**	0	**0%**	0	**0%**	0
6	Datacenter Security	9	9	**100%**	0	**0%**	0	**0%**	0	**0%**	0
7	Encryption & Key Management	4	4	**100%**	0	**0%**	0	**0%**	0	**0%**	0
8	Governance and Risk Management	12	12	**100%**	0	**0%**	0	**0%**	0	**0%**	0
9	Human Resources	12	12	**100%**	0	**0%**	0	**0%**	0	**0%**	0
10	Identity & Access Management	13	13	**100%**	0	**0%**	0	**0%**	0	**0%**	0
11	Infrastructure & Virtualization Security	12	9	**75%**	3	**25%**	3	**25%**	0	**0%**	0
12	Interoperability & Portability	5	2	**40%**	3	**60%**	1	**20%**	2	**40%**	0
13	Mobile Security	20	15	**75%**	5	**25%**	2	**10%**	3	**15%**	0
14	Security Incident Management, E-Discovery & Cloud Forensics	5	5	**100%**	0	**0%**	0	**0%**	0	**0%**	0
15	Supply Chain Management, Transparency and Accountability	9	9	**100%**	0	**0%**	0	**0%**	0	**0%**	0
16	Threat and Vulnerability Management	3	3	**100%**	0	**0%**	0	**0%**	0	**0%**	0
	TOTAL	**136**	**124**	**91%**	**12**	**9%**	**7**	**5%**	**5**	**4%**	**1**

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

[2] As the STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

7.3 Snapshot of Differences between Level of MTCS SS

Of the identified gaps, the table below summarises the 12 common gaps identified for MTCS SS Levels 1, 2 and 3:

CSA CCM Topic	CSA CCM Sub-topic	No.	CSA CCM Control ID
Application & Interface Security	Customer Access Requirements	1	AIS-02
Infrastructure & Virtualization Security	Management - Vulnerability Management	2	IVS-05
	VM Security - vMotion Data Protection	3	IVS-10
	Wireless Security	4	IVS-12
Interoperability & Portability	APIs	5	IPY-01
	Policy & Legal	6	IPY-03
	Virtualization	7	IPY-05
Mobile Security	Device Management	8	MOS-10
	Jailbreaking and Rooting	9	MOS-12
	Policy	10	MOS-17
	Remote Wipe	11	MOS-18
	Security Patches	12	MOS-19

Of the remainder, Cloud Service Providers certified to MTCS SS Level 2 or above may disregard the following[1]:

CSA CCM Topic	CSA CCM Sub-topic	No.	CSA CCM Control ID
Data Security & Information Lifecycle Management	Information Leakage	1	DSI-05
Governance and Risk Management	Baseline Requirements	2	GRM-01

[1] These are relevant for MTCS SS Level 1

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 "CSA CCM V3.0 Control ID / Control Name" specifies the controls that are currently stated in the CSA CCM.

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 MTCS SS clauses” specifies the clauses that are currently stated in the MTCS SS and have equal requirements or components relevant to the corresponding CSA CCM controls specified under the column “CSA CCM V3.0 Control ID / Control Name”.

4) The column “Reference to matching MTCS SS sub-clauses” specifies the sub-clauses that are currently stated in the MTCS SS and have equal requirements or components relevant to the corresponding CSA CCM controls specified under the column “CSA CCM V3.0 Control ID / Control Name”. The corresponding parent clauses of these sub-clauses can be found under the column “Reference to matching MTCS SS clauses”.

5) The column “Remarks on identified gaps” denotes observations and additional notes based on the gap analysis.

As the STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, 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.

Additionally, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

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’.

It is recommended for Cloud Service Providers to view the complete set of requirements listed in the CSA CCM for the authoritative list of requirements.

Additionally, Cloud Service Providers shall determine the boundaries and applicability of the information security management system to establish its scope.

9 Gap Analysis

The purpose of this section is to list the differences between CSA CCM and MTCS SS describing gaps discovered in each control area and their respective clauses. The table below summarises the list of requirements in CSA CCM and the respective classification of gaps in relation to MTCS SS Levels 1, 2 and 3 requirements.

As the STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, 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 under the column "Remarks on identified gaps".

Additionally, where applicable, there will be common gaps when mapping MTCS SS to CSA CCM, and MTCS SS to ISO/IEC 27001:2013. Users of this report are advised to take into consideration of the number of common gaps so as to avoid duplication in efforts to remediate gaps.

Where level is not specified (e.g., AIS-02) under the column "Gaps", the gap applies to all MTCS SS Levels. Refer to DSI-05 for a scenario where there are differences in gaps across the 3 levels.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
AIS Application & Interface Security				
AIS-01 Application Security	INCLUDED	16 System acquisitions and development	16.1 Development, acquisition and release management	N.A
AIS-02 Customer Access Requirements	INCREMENTAL	23 Cloud user access	23.1 User access registration	While MTCS SS defines the controls to address security, contractual and regulatory requirements in general; it does not specifically require that the identified requirements must be addressed prior to granting access to customers. Note: Gap is also found when mapping MTCS SS to ISO/IEC 27001:2013. Refer to Clause A.9.4.1 in ISO/IEC 27001:2013.
AIS-03 Data Integrity	INCLUDED	12 Data governance 16 System acquisitions and development	12.3 Data integrity 16.1 Development, acquisition and release management	MTCS SS Level 1 has no applicable control requirements to address data integrity for data output.
AIS-04 Data Security / Integrity	INCLUDED	6 Information security management 10 Legal and compliance 16 System acquisitions and development	6.1 Information security management system (ISMS) 6.4 Information security policy 10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 16.1 Development, acquisition and release management	N.A
Audit Assurance & Compliance				
AAC-01 Audit Planning	INCLUDED	6 Information security management	6.6 Information security audits	N.A
AAC-02 Independent Audits	INCLUDED	6 Information security management 10 Legal and compliance 18 Physical and environmental	6.6 Information security audits 10.2 Compliance with policies and standards 18.6 Physical security review	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
AAC-03 Information System Regulatory Mapping	INCLUDED	6 Information security management 10 Legal and compliance	6.4 Information security policy 10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards	N.A
Business Continuity Management & Operational Resilience				
BCR-01 Business Continuity Planning	INCLUDED	19 Operations 21 Business continuity planning (BCP) and disaster recovery (DR)	19.2 Documentation of service operations and external dependencies 21.1 BCP framework 21.2 BCP and DR plans	N.A
BCR-02 Business Continuity Testing	INCLUDED	11 Incident management 21 Business continuity planning (BCP) and disaster recovery (DR)	11.2 Information security incident response plan testing and updates 21.3 BCP and DR testing	N.A
BCR-03 Datacenter Utilities / Environmental conditions	INCLUDED	18 Physical and environment	18.1 Asset management 18.5 Environmental threats and equipment power failures	N.A
BCR-04 Documentation	INCLUDED	19 Operations 21 Business continuity planning (BCP) and disaster recovery (DR)	19.1 Operations management policies and procedures 19.2 Documentation of service operations and external dependencies 21.2 BCP and DR plans	MTCS SS Level 1 does not specifically require system documentation such as administrator guides, user guides, and architecture diagrams, to be made available for authorised personnel. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
BCR-05 Environmental Risks	INCLUDED	18 Physical and environment	18.5 Environmental threats and equipment power failures	N.A
BCR-06 Equipment Location	INCLUDED	18 Physical and environmental 21 Business continuity planning (BCP) and disaster recovery (DR)	18.5 Environmental threats and equipment power failures 21.2 BCP and DR plans	N.A
BCR-07 Equipment Maintenance	INCLUDED	18 Physical and environmental	18.1 Asset management	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
BCR-08 Equipment Power Failures	INCLUDED	18 Physical and environment	18.1 Asset management 18.5 Environmental threats and equipment power failures	N.A
BCR-09 Impact Analysis	INCLUDED	8 Risk management 19 Operations 21 Business continuity planning (BCP) and disaster recovery (DR)	8.2 Risk assessment 19.2 Documentation of service operations and external dependencies 21.1 BCP framework 21.2 BCP and DR plans	N.A
BCR-10 Management Program	INCLUDED	21 Business continuity planning (BCP) and disaster recovery (DR)	21.1 BCP framework 21.2 BCP and DR plans	N.A
BCR-11 Policy	INCLUDED	6 Information security management 7 Human resources 8 Risk Management 11 Incident management 19 Operations	6.1 Information security management system (ISMS) 7.6 Information security training and awareness 8.2 Risk Assessment 11.2 Information security incident response plan testing and updates 19.2 Documentation of service operations and external dependencies	N.A
BCR-12 Retention Policy	INCLUDED	12 Data governance 19 Operations 21 Business continuity planning (BCP) and disaster recovery (DR)	12.6 Data retention 12.7 Data backups 19.6 Recoverability 21.1 BCP framework	MTCS SS Level 1 has no applicable control requirements that address data retention policy and procedures. While testing of business continuity plan is covered in general in MTCS SS Level 1, specific requirement to test backup capabilities is only covered in MTCS SS Level 2. Note: ISO/IEC 27001:2013 covers this requirement under Section A.12.3.
Change Control & Configuration Management				
CCC-01 New Development / Acquisition	INCLUDED	16 System acquisitions and development	16.1 Development, acquisition and release management	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
CCC-02 Outsourced Development	INCLUDED	14 Secure configuration 16 System acquisitions and development	14.2 Malicious code prevention 16.1 Development, acquisition and release management 16.4 Source code security 16.5 Outsourced software development	N.A
CCC-03 Quality Testing	INCLUDED	15 Security testing and monitoring 16 System acquisitions and development	15.1 Vulnerability scanning 15.2 Penetration testing 16.1 Development, acquisition and release management 16.5 Outsourced software development	N.A
CCC-04 Unauthorized Software Installations	INCLUDED	14 Secure configuration 16 System acquisitions and development	14.8 Unauthorised software 16.1 Development, acquisition and release management	N.A
CCC-05 Production Changes	INCLUDED	9 Third party 14 Secure configuration 16 System acquisitions and development 20 Change management 23 Cloud user access	9.4 Third party delivery management 14.1 Server and network device configuration standards 14.2 Malicious code prevention 16.1 Development, acquisition and release management 20.1 Change management process 20.2 Backup procedures 20.3 Back-out or rollback procedures 23.10 Communication with cloud users	N.A
Data Security & Information Lifecycle Management				

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
DSI-01 Classification	INCLUDED	10 Legal and compliance 12 Data governance	10.1 Compliance with regulatory and contractual requirements 12.1 Data classification	While MTCS SS Level 1 requires compliance with regulatory and contractual requirements in general, it has no applicable controls on data classification. Note: ISO/IEC 27001:2013 covers this requirement under Section A.8.2.
DSI-02 Data Inventory / Flows	INCLUDED	6 Information security management 9 Third party 12 Data governance 24 Tenancy and customer isolation	6.1 Information security management systems (ISMS) 9.3 Third party agreement 12.1 Data classification 12.2 Data ownership 12.5 Data protection 12.4 Data labelling / handling 12.10 Tracking of data 24.1 Multi tenancy 24.3 Network protection	While MTCS SS Level 1 covers third party agreements and protection for media in general, it has no applicable controls on data inventory. It also does not explicitly require the provider to inform customers, upon request, of the compliance impact and risk if customer data is used as part of the services. While the documentation of data ownership implies some form of data inventory, MTCS SS Levels 2 and 3 do not cover the documentation of data flow. It also does not specifically require the provider to inform customers, upon request, of the compliance impact and risk if customer data is used as part of the services. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.8.1, A.8.2 and A.8.3.
DSI-03 eCommerce Transactions	INCLUDED	17 Encryption	17.2 Channel encryption	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
DSI-04 Handling / Labeling / Security Policy	INCLUDED	6 Information security management 12 Data governance	6.8 Acceptable usage 12.1 Data classification 12.4 Data labelling / handling 12.7 Data backups	While MTCS SS covers data labelling and handling, it does not specifically require a mechanism in place for label inheritance for objects that act as aggregate containers for data. Note: ISO/IEC 27001:2013 covers this requirement under Section A.8.2.
DSI-05 Information Leakage	Level 1: INCREMENTAL	12 Data governance	12.5 Data protection	MTCS SS Level 1 does not have requirement that specifically address data leakage. Note: Gap is also found when mapping MTCS SS to ISO/IEC 27001:2013. Refer to Clause 7.5.3(para.2d) in ISO/IEC 27001:2013.
	Level 2: INCLUDED			N.A
	Level 3: INCLUDED			
DSI-06 Non-Production Data	INCLUDED	16 System acquisitions and development 22 Cloud services administration	16.3 System testing 22.10 Segregation of duties	N.A
DSI-07 Ownership / Stewardship	INCLUDED	6 Information security management 12 Data governance	6.2 Management of information security 12.2 Data ownership	MTCS SS Level 1 does not cover data ownership. Note: ISO/IEC 27001:2013 covers this requirement under Section A.8.1.
DSI-08 Secure Disposal	INCLUDED	12 Data governance	12.5 Data protection 12.8 Secure disposal and decommissioning of hardcopy, media and equipment	N.A
Datacenter Security				
DCS-01 Asset Management	INCLUDED	18 Physical and environment	18.1 Asset management	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
DCS-02 Controlled Access Points	INCLUDED	14 Secure configuration 18 Physical and environment	14.4 Physical port protection 18.3 Physical access 18.4 Visitors 18.6 Physical security review	N.A
DCS-03 Equipment Identification	INCLUDED	22 Cloud services administration	22.7 Administrator access security	N.A
		6 Information security management 22 Cloud services administration	6.8 Acceptable usage 22.7 Administrator access security	N.A
DCS-04 Off-Site Authorization	INCLUDED	18 Physical and environment	18.2 Off-site movement	N.A
DCS-05 Off-Site Equipment	INCLUDED	12 Data governance 18 Physical and environment	12.8 Secure disposal and decommissioning of hardcopy, media and equipment 18.1 Asset management	N.A
DCS-06 Policy	INCLUDED	6 Information security management 18 Physical and environment	6.1 Information security management system (ISMS) 18.1 Asset management 18.3 Physical access 18.5 Environmental threats and equipment power failures	N.A
DCS-07 Secure Area Authorization	INCLUDED	18 Physical and environment	18.3 Physical access 18.4 Visitors	N.A
DCS-08 Unauthorized Persons Entry	INCLUDED	18 Physical and environment	18.3 Physical access 18.4 Visitors	N.A
DCS-09 User Access	INCLUDED	14 Secure configuration 18 Physical and environment	14.4 Physical port protection 18.3 Physical access 18.4 Visitors 18.5 Environmental threats and equipment power failures	N.A
Encryption & Key Management				
EKM-01 Entitlement	INCLUDED	17 Encryption 22 Cloud services administration 23 Cloud user access	17.3 Key management 22.1 Privilege account creation 23.1 User access registration	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
EKM-02 Key Generation	INCLUDED	10 Legal and compliance 17 Encryption	10.4 Use of compliant cryptography controls 17.1 Encryption policies and procedures 17.3 Key management	While MTCS SS covers cryptographic key lifecycle management in general, it does not explicitly require Cloud Service Providers to inform the customers of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibilities over implementation of the controls. Note: ISO/IEC 27001:2013 covers this requirement under Section A.10.1.
EKM-03 Sensitive Data Protection	INCLUDED	10 Legal and compliance 17 Encryption 24 Tenancy and customer isolation	10.4 Use of compliant cryptography controls 17.1 Encryption policies and procedures 17.2 Channel encryption 17.3 Key management 17.4 Electronic messaging security 24.3 Network protection	N.A
EKM-04 Storage and Access	INCLUDED	10 Legal and compliance 17 Encryption	10.4 Use of compliant cryptography controls 17.3 Key management	While MTCS SS covers the application of industry practices in cryptographic controls and the storage of cryptographic keys in general, it does not specifically require keys not to be stored in the cloud but maintained by the cloud consumer or trusted key management provider. It also does not mention key management and key usage are to be separated duties. Note: ISO/IEC 27001:2013 covers this requirement under Section A.10.1.
Governance and Risk Management				

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
GRM-01 Baseline Requirements	Level 1: INCREMENTAL	14 Secure configuration 16 System acquisitions and development	14.1 Server and network device configuration standards 14.9 Enforcement checks 16.1 Development, acquisition and release management	While MTCS SS Level 1 requires compliance checks to be done regularly, it does not specify the frequency of such checks.
	Level 2: INCLUDED			N.A
	Level 3: INCLUDED			
GRM-02 Data Focus Risk Assessments	INCLUDED	8 Risk management 12 Data governance 24 Tenancy and customer isolation	8.1 Risk management programme 8.2 Risk assessment 12.8 Secure disposal and decommissioning of hardcopy, media and equipment 24.4 Virtualisation	N.A
GRM-03 Management Oversight	INCLUDED	6 Information security management 7 Human resources	6.1 Information security management system (ISMS) 6.2 Management of information security 6.3 Management oversight of information security 7.6 Information security training and awareness	N.A
GRM-04 Management Program	INCLUDED	6 Information security management 8 Risk management 23 Cloud user access	6.1 Information security management system (ISMS) 6.2 Management of information security 8.1 Risk management programme 23.5 User password reset and first logon change 23.6 Password protection 23.7 User session management	N.A
GRM-05 Management Support / Involvement	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.2 Management of information security 6.3 Management oversight of information security	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
GRM-06 Policy	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.2 Management of information security 6.4 Information security policy	N.A
GRM-07 Policy Enforcement	INCLUDED	7 Human resources	7.3 Employment and contract terms and conditions 7.4 Disciplinary process	N.A
GRM-08 Policy Impact on Risk Assessments	INCLUDED	6 Information security management 8 Risk management 15 Security testing and monitoring 24 Tenancy and customer isolation	6.1 Information security management system (ISMS) 8.2 Risk assessment 15.3 Security monitoring 24.4 Virtualisation	N.A
GRM-09 Policy Reviews	INCLUDED	6 Information security management	6.5 Review of information security policy	N.A
GRM-10 Risk Assessments	INCLUDED	6 Information security management 8 Risk management	6.1 Information security management system (ISMS) 8.1 Risk management programme 8.2 Risk assessment	N.A
GRM-11 Risk Management Framework	INCLUDED	6 Information security management 8 Risk management	6.3 Management oversight of information security 8.1 Risk management programme 8.3 Risk management	N.A
GRM-12 Risk Mitigation / Acceptance	INCLUDED	6 Information security management 8 Risk management	6.1 Information security management system (ISMS) 8.1 Risk management programme 8.3 Risk management 8.4 Risk register	MTCS SS Level 1 does not specifically require the establishment of risk acceptance levels based on risk criteria. Note: ISO/IEC 27001:2013 covers this requirement under Section 6.1.
Human Resources				

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
HRS-01 Asset Returns	INCLUDED	7 Human resources	7.3 Employment and contract terms and conditions 7.5 Asset returns	N.A
HRS-02 Background Screening	INCLUDED	7 Human resources 9 Third party	7.1 Background screening	N.A
HRS-03 Employment Agreements	INCLUDED	7 Human resources 9 Third party	7.3 Employment and contract terms and conditions	N.A
HRS-04 Employment Termination	INCLUDED	7 Human resources 22 Cloud services administration	7.3 Employment and contract terms and conditions 22.3 Administrator access review and revocation	MTCS SS Level 1 does not explicitly require the roles and responsibilities for personnel executing the employment termination or change in employment procedures to be established, documented and made known to relevant parties. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.7.2 and A.7.3.
HRS-05 Industry Knowledge / Benchmarking	INCLUDED	6 Information security management	6.7 Information security liaisons (ISL)	N.A
HRS-06 Mobile Device Management	INCLUDED	6 Information security management	6.8 Acceptable usage	While MTCS SS covers the acceptable usage of technologies and devices in general, it does not have specific requirements for mobile devices as required by CCM Control HRS-06. Note: ISO/IEC 27001:2013 covers this requirement under Section A.6.2.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
HRS-07 Non-Disclosure Agreements	INCLUDED	7 Human resources 9 Third party	7.3 Employment and contract terms and conditions 9.3 Third party agreement	While MTCS SS requires employees to sign terms and conditions of their employment, it does not explicitly require controls for signed non-disclosure or confidentiality agreements, and conducting periodical reviews on the subject. Note: ISO/IEC 27001:2013 covers this requirement under Section A.13.2.
HRS-08 Roles / Responsibilities	INCLUDED	6 Information security management	6.2 Management of information security 6.4 Information security policy	N.A
HRS-09 Technology Acceptable Use	INCLUDED	6 Information security management 10 Legal and compliance	6.8 Acceptable usage 10.3 Prevention of misuse of cloud facilities	N.A
HRS-10 Training / Awareness	INCLUDED	7 Human resources 10 Legal and compliance	7.6 Information security training and awareness 10.3 Prevention of misuse of cloud facilities	N.A
HRS-11 User Responsibility	INCLUDED	6 Information security management 7 Human resources	6.8 Acceptable usage 7.3 Employment and contract terms and conditions	N.A
HRS-12 Workspace	INCLUDED	10 Legal and compliance 18 Physical and environmental	10.2 Compliance with policies and standards 18.1 Asset management	N.A
Identity & Access Management				
IAM-01 Audit Tools Access	INCLUDED	6 Information security management 13 Audit logging and monitoring 22 Cloud services administration	6.6 Information security audits 13.3 Audit trails 22.8 Administrator access logs	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IAM-02 Credential Lifecycle / Provision Management	INCLUDED	6 Information security management 10 Legal and compliance 22 Cloud services administration 23 Cloud user access 24 Tenancy and customer isolation	6.2 Management of information security 10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 22.1 Privilege account creation 22.3 Administrator access review and revocation 22.4 Account lockout 22.5 Password change 22.6 Password reset and first logon 22.7 Administrator access security 22.9 Session management 22.12 Third party administrative access 22.13 Service and application accounts 23.1 User access registration 23.2 User access security 23.4 User account lockout 23.9 Self-service portal creation and management of user accounts 24.1 Multi tenancy 24.3 Network protection 24.5 Storage area networks (SAN)	N.A
IAM-03 Diagnostic / Configuration Ports Access	INCLUDED	14 Secure configuration	14.4 Physical port protection	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IAM-04 Policies and Procedures	INCLUDED	6 Information security management 23 Cloud user access 24 Tenancy and customer isolation	6.4 Information security policy 22.1 Privilege account creation 22.3 Administrator access review and revocation 23.1 User access registration 23.2 User access security 24.3 Network protection	N.A
IAM-05 Segregation of Duties	INCLUDED	22 Cloud services administration	22.1 Privilege account creation 22.10 Segregation of duties 22.12 Third party administrative access	N.A
IAM-06 Source Code Access Restriction	INCLUDED	16 System acquisitions and development 23 Cloud user access	16.4 Source code security 23.1 User access registration	N.A
IAM-07 Third Party Access	INCLUDED	9 Third party 22 Cloud Services administration 24 Tenancy and customer isolation	9.1 Third party due diligence 9.2 Identification of risks related to third parties 22.12 Third party administrative access 24.3 Network protection	N.A
IAM-08 Trusted Sources	INCLUDED	22 Cloud services administration 23 Cloud user access 24 Tenancy and customer isolation	22.12 Third party administrative access 23.1 User access registration 24.5 Storage area networks (SAN)	N.A
IAM-09 User Access Authorization	INCLUDED	22 Cloud services administration 23 Cloud user access	22.1 Privilege account creation 23.1 User access registration 23.2 User access security	While MTCS SS defines the controls to restrict user access to authorised personnel only, it does not require customers to be informed of this user access, especially in scenarios where customer data is used and / or customer has some shared responsibility over the implementation of controls. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.2.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IAM-10 User Access Reviews	INCLUDED	22 Cloud services administration	22.3 Administrator access review and revocation 22.10 Segregation of duties	N.A
IAM-11 User Access Revocation	INCLUDED	7 Human resources 22 Cloud services administration	7.3 Employment and contract terms and conditions 22.3 Administrator access review and revocation	While MTCS SS defines the controls to timely de-provision user access, it does not require customers to be informed of these changes, especially in scenarios where customer data is used and / or customer has some shared responsibility over the implementation of controls. Note: ISO/IEC 27001:2013 covers this requirement under Section A.9.2.
IAM-12 User ID Credentials	INCLUDED	22 Cloud services administration 23 Cloud user access 24 Tenancy and customer isolation	22.1 Privilege account creation 23.1 User access registration 23.2 User access security 23.9 Self-service portal creation and management of user accounts 24.3 Network protection	N.A
IAM-13 Utility Programs Access	INCLUDED	14 Secure configuration	14.5 Restrictions to system utilities	N.A
Infrastructure & Virtualization Security				
IVS-01 Audit Logging / Intrusion Detection	INCLUDED	10 Legal and compliance 13 Audit logging and monitoring 15 Security testing and monitoring 23 Cloud user access	10.3 Prevention of misuse of cloud facilities 10.6 Continuous compliance monitoring 13.1 Logging and monitoring process 13.2 Log review 13.3 Audit trails 13.4 Backup and retention of audit trails 13.5 Usage logs 15.3 Security monitoring 23.2 User access security	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IVS-02 Change Detection	INCLUDED	12 Data governance 13 Audit logging and monitoring 14 Secure configuration 24 Tenancy and customer isolation	13.1 Logging and monitoring process 14.8 Unauthorised software 24.1 Multi tenancy 24.4 Virtualisation	N.A
IVS-03 Clock Synchronization	INCLUDED	13 Audit logging and monitoring	13.1 Logging and monitoring process	N.A
IVS-04 Information System Documentation	INCLUDED	19 Operations 24 Tenancy and customer isolation	19.3 Capacity management 24.4 Virtualisation	N.A
IVS-05 Management - Vulnerability Management	INCREMENTAL	6 Information security management 24 Tenancy and customer isolation	6.1 Information security management system (ISMS) 24.3 Network protection 24.4 Virtualisation	While MTCS SS covers vulnerability management for virtualised technologies in general, it does not specifically require the security vulnerability assessment tools or services used by the Cloud Service Provider to manage vulnerabilities of virtualisation to accommodate the virtualisation technologies used.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IVS-06 Network Security	INCLUDED	10 Legal and compliance 13 Audit logging and monitoring 14 Secure configuration 15 Security testing and monitoring 16 System acquisitions and development 20 Change management 22 Cloud services administration 23 Cloud user access 24 Tenancy and customer isolation	10.6 Continuous compliance monitoring 13.2 Log review 14.1 Server and network device configuration standards 14.4 Physical port protection 14.6 System and network session management 14.7 Unauthorised service and protocols 15.3 Security monitoring 16.1 Development, acquisition and release management 20.4 Separation of environment 22.7 Administrator access security 23.2 User access security 24.1 Multi tenancy 24.3 Network protection 24.4 Virtualisation 24.5 Storage area networks (SAN)	N.A
IVS-07 OS Hardening and Base Controls	INCLUDED	14 Secure configuration 20 Change management 24 Tenancy and customer isolation	14.1 Server and network device configuration standards 14.2 Malicious code prevention 14.4 Physical port protection 14.7 Unnecessary service and protocols 20.5 Patch management procedures 24.4 Virtualisation	N.A
IVS-08 Production / Non-Production Environments	INCLUDED	16 System acquisitions and development 20 Change management 22 Cloud services administration 24 Tenancy and customer isolation	16.1 Development, acquisition and release management 20.4 Separation of environment 22.10 Segregation of duties 24.1 Multi tenancy	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IVS-09 Segmentation	INCLUDED	24 Tenancy and customer isolation	24.1 Multi tenancy 24.2 Supporting infrastructure segmentation 24.3 Network protection 24.4 Virtualisation	N.A
IVS-10 VM Security - vMotion Data Protection	INCREMENTAL	6 Information security management 17 Encryption 24 Tenancy and customer isolation	6.1 Information security management system (ISMS) 17.2 Channel encryption 24.4 Virtualisation	While MTCS SS covers channel encryption in general for channels used for transmission of sensitive information, it does not specifically require the usage of secure and encrypted channels for migrating physical servers, applications, or data to virtualised servers.
IVS-11 VMM Security - Hypervisor Hardening	INCLUDED	13 Audit logging and monitoring 14 Secure configuration 17 Encryption 22 Cloud services administration 24 Tenancy and customer isolation	13.1 Logging and monitoring process 14.1 Server and network device configuration standards 17.2 Channel encryption 22.7 Administrator access security 22.11 Secure transmission of access credentials 24.3 Network protection 24.4 Virtualisation	N.A
IVS-12 Wireless Security	INCREMENTAL	14 Secure configuration 18 Physical and environmental 23 Cloud user access 24 Tenancy and customer isolation	14.1 Server and network device configuration standards 18.3 Physical access 23.3 User access password 23.5 User password reset and first logon change 24.3 Network protection	MTCS SS relies on network segmentation and physical security; hence it does not specifically require the capability to detect unauthorised wireless network devices and timely disconnection from the network.
Interoperability & Portability				

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IPY-01 APIs	INCREMENTAL	16 System acquisitions and development	16.1 Development, acquisition and release management	While MTCS SS covers software development in accordance with industry standards and practices, it does not specifically require utilisation of open and published APIs to maximise interoperability.
IPY-02 Data Request	INCLUDED	N.A	N.A	MTCS SS does not require unstructured data to be made available to the customers and provided to them upon request in an industry-standard format (e.g., .doc, .xls, or .pdf). However, MTCS SS requires Cloud Service Providers to complete, in addition to the implementation requirements, a service provider disclosure form to specify whether such documentation and information are made available to the cloud users. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
IPY-03 Policy & Legal	NEW	N.A	N.A	MTCS SS does not require providers to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability. It also does not require the providers to satisfy customer (tenant) requirements on portability for application development and information exchange, usage and integrity persistence.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
IPY-04 Standardized Network Protocols	INCLUDED	N.A	N.A	MTCSS does not define controls to make available a document for consumers (tenants) detailing the relevant interoperability and portability standards that are involved. Note: ISO/IEC 27001:2013 covers this requirement under Section 7.5.
IPY-05 Virtualization	NEW	N.A	N.A	MTCS SS does not require providers to use an industry-recognised virtualisation platform and standard virtualisation formats (e. g., OVF) to help ensure interoperability between varying environments and infrastructures. It also does not require providers to have documented custom changes made to any hypervisor in use, and have all solution-specific virtualisation hooks available for customer review.
Mobile Security				
MOS-01 Anti-Malware	INCLUDED	7 Human resources 14 Secure configuration	7.6 Information security awareness and training 14.2 Malicious code prevention	MTCS SS does not explicitly require anti-malware awareness training specific to mobile devices, to be included as one of the topics of information security awareness and training. Mobile devices would typically not be part of MTCS SS scope. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2 and A.12.2.
MOS-02 Application Stores	INCLUDED	6 Information security management	6.8 Acceptable usage	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
MOS-03 Approved Applications	INCLUDED	6 Information security management 14 Secure configuration	6.8 Acceptable usage 14.8 Unauthorised software	N.A
MOS-04 Approved Software for BYOD	INCLUDED	7 Human resources	7.6 Information security training and awareness	While MTCS SS covers awareness and training in general, it does not define the controls on BYOD policy and supporting awareness training sessions. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2 and A.6.2.
MOS-05 Awareness and Training	INCLUDED	6 Information security management 7 Human resources	6.8 Acceptable usage 7.6 Information security training and awareness	While MTCS SS covers acceptable usage for technologies, services and devices in general, it does not specifically require the establishment of a mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. Also, MTCS SS does not specifically require the communication of such a policy and its corresponding requirements through the company's security awareness and training program. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.2 and A.6.2.
MOS-06 Cloud Based Services	INCLUDED	6 Information security management	6.8 Acceptable usage	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
MOS-07 Compatibility	INCLUDED	20 Change management	20.1 Change management process	While MTCS SS requires testing for compatibility issues in general, it does not explicitly require a documented application validation process to be established. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.5 and A.6.2.
MOS-08 Device Eligibility	INCLUDED	N.A	N.A	MTCS SS does not require a Bring-Your-Own-Device (BYOD) policy to be developed and documented. Note: ISO/IEC 27001:2013 covers this requirement under Sections 7.5 and A.6.2.
MOS-09 Device Inventory	INCLUDED	18 Physical and environmental	18.1 Asset management	While MTCS SS requires the establishment and maintenance of an inventory of assets, it does not specifically require mobile devices used to store and access company data to be included in such an inventory, and the inclusion of the mobile devices' status details as stated in CCM Control MOS-09. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.6.2 and A.8.1.
MOS-10 Device Management	NEW	N.A	N.A	MTCS SS does not require a centralised mobile device management solution to be deployed to all mobile devices used to store, transmit, or process company data.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
MOS-11 Encryption	INCLUDED	10 Legal and compliance 12 Data Governance 17 Encryption	10.4 Use of compliant cryptography controls 12.5 Data protection 17.1 Encryption policies and procedures	MTCS SS does not specifically require the establishment of a mobile device policy. Therefore, requirements for the usage of cryptographic controls on mobile devices are not included. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.6.2 and A.10.1.
MOS-12 Jailbreaking and Rooting	NEW	N.A	N.A	MTCS SS does not require the prohibition of circumvention of built-in security controls on mobile devices.
MOS-13 Legal	INCLUDED	6 Information security management	6.8 Acceptable usage	While MTCS SS requires policies for acceptable usage in general, it does not specifically require a BYOD policy which includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. Note: ISO/IEC 27001:2013 covers this requirement under Section A.6.2.
MOS-14 Lockout Screen	INCLUDED	14 Secure configuration 22 Cloud services administration	14.6 System and network session management 22.4 Account lockout 22.9 Session management	N.A
MOS-15 Operating Systems	INCLUDED	20 Change management	20.1 Change management process	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
MOS-16 Passwords	INCLUDED	22 Cloud services administration	22.2 Generation of administrator passwords 22.5 Password change 22.6 Password reset and first logon	MTCS SS does not specifically require the establishment of a mobile device policy. Therefore, the requirements on the documentation and enforcement of password policies on mobile devices are consequently not included. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.6.2 and A.9.4.
MOS-17 Policy	INCREMENTAL	6 Information security management	6.8 Acceptable usage	While MTCS SS requires policies for acceptable usage in general, it does not specifically require a BYOD policy covering requirements for the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and use of anti-malware software.
MOS-18 Remote Wipe	NEW	N.A	N.A	MTCS SS does not require mobile devices to have the capability to be remotely wiped by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.
MOS-19 Security Patches	INCREMENTAL	20 Change management	20.5 Patch management procedures	While MTCS SS requires the establishment of patch management procedures in general, it does not specifically require mobile devices to allow remote validation to download the latest security patches by company IT personnel.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
MOS-20 Users	INCLUDED	6 Information security management	6.8 Acceptable usage	MTCS SS does not require the establishment and documentation of a BYOD policy. Therefore, details with regards to the clarification of the systems and servers allowed for use or access on a BYOD-enabled device are consequently not included. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.6.2, A.8.2 and A.8.3.
Security Incident Management, E-Discovery & Cloud Forensics				
SEF-01 Contact / Authority Maintenance	INCLUDED	6 Information security management 11 Incident management	6.7 Information security liaisons (ISL) 11.1 Information security incident response plan and procedures	N.A
SEF-02 Incident Management	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures 11.4 Problem management	N.A
SEF-03 Incident Reporting	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures 11.3 Information security incident reporting	N.A
SEF-04 Incident Response Legal Preparation	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures	N.A
SEF-05 Incident Response Metrics	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures 11.3 Information security incident reporting 11.4 Problem management	N.A
Supply Chain Management, Transparency and Accountability				

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
STA-01 Data Quality and Integrity	INCLUDED	9 Third Party 12 Data governance 22 Cloud services administration	9.1 Third party due diligence 9.4 Third party delivery management 12.3 Data integrity 22.10 Segregation of duties	MTCS SS Level 1 does not include requirements that cover data quality/integrity. While MTCS SS Levels 2 and 3 have controls to address data integrity in general, it does not specifically require providers to inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. Note: ISO/IEC 27001:2013 covers this requirement under Sections 6.1 and A.10.1.
STA-02 Incident Reporting	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures 11.3 Information security incident reporting	N.A
STA-03 Network / Infrastructure Services	INCLUDED	9 Third Party 14 Secure configuration 16 System acquisitions and development 19 Operations	9.4 Third party delivery management 14.1 Server and network device configuration standards 16.1 Development, acquisition and release management 19.4 Service levels	While MTCSS SS defines controls to develop and implement standard policies and processes across its entire infrastructure, it does not explicitly require defining and deploying as per the agreed service levels. The same has been incorporated in MTCS SS Levels 2 and 3. Note: ISO/IEC 27001:2013 covers this requirement under Section A.15.1.
STA-04 Provider Internal Assessments	INCLUDED	6 Information security management 10 Legal and compliance	6.6 Information security audits 10.2 Compliance with policies and standards	N.A

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
STA-05 Supply Chain Agreements	INCLUDED	9 Third party 19 Operations	9.3 Third party agreement 19.4 Service levels	While MTCS SS has controls to address service levels in general, additional details as specified in CCM Control STA-05 are not fully covered. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.15.1 and A.15.2.
STA-06 Supply Chain Governance Reviews	INCLUDED	9 Third party	9.1 Third party due diligence 9.2 Identification of risk related to third parties 9.4 Third party delivery management	While MTCS SS Level 1 has requirements for providers to ensure practices of their partners are consistent and aligned with contractual and legal agreements, it does not specifically require regular reviews to be performed. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.15.1 and A.15.2.
STA-07 Supply Chain Metrics	INCLUDED	9 Third party 10 Legal and compliance	9.4 Third party delivery management 9.3 Third party agreement 10.5 Third party compliance	While MTCS SS Levels 1 and 2 cover the management of service delivery with third parties in general, it does not specifically require the establishment of abilities to measure and address non-conformance of provisions and / or terms across the entire supply chain, and for managing service-level conflicts or inconsistencies resulting from disparate supplier relationships. Note: ISO/IEC 27001:2013 covers this requirement under Sections A.15.1 and A.15.2.

CSA CCM V3.0 Control ID / Control Name	Gaps	Reference to matching MTCS SS clauses	Reference to matching MTCS SS sub-clauses	Remarks on identified gaps
STA-08 Third Party Assessment	INCLUDED	6 Information security management 9 Third party	6.2 Management of information security 9.4 Third party delivery management	While MTCS SS Level 1 covers the assurance of third party services, monitoring and regular review are only specifically mentioned from MTCS SS Level 2. Note: ISO/IEC 27001:2013 covers this requirement under Section A.15.2.
STA-09 Third Party Audits	INCLUDED	9 Third party 10 Legal and compliance	9.2 Identification of risk related to third parties 9.4 Third party delivery management 10.5 Third party compliance	While MTCS SS Level 1 covers the assurance of third party services, monitoring and regular review are only specifically mentioned from MTCS SS Level 2. Note: ISO/IEC 27001:2013 covers this requirement under Section A.15.2.
Threat and Vulnerability Management				
TVM-01 Anti-Virus / Malicious Software	INCLUDED	14 Secure configuration	14.2 Malicious code prevention	N.A
TVM-02 Vulnerability / Patch Management	INCLUDED	6 Information security management 15 Security testing and monitoring 20 Change management	6.7 Information security liaisons (ISL) 15.1 Vulnerability scanning 15.2 Penetration Testing 15.3 Security Monitoring 16.1 Development, acquisition and release management 20.5 Patch management procedures	While MTCS SS defines controls to establish process for identification and risk-based mitigation of vulnerabilities, it does not require customers to be informed of policies and processes, especially in scenarios where customer data is used and/or customer has some shared responsibility over implementation of control. Note: ISO/IEC 27001:2013 covers this requirement under Sections 4.2, 4.3 and 7.4.
TVM-03 Mobile Code	INCLUDED	14 Secure configuration	14.2 Malicious Code Prevention 14.3 Portable code	N.A

<End of Gap Analysis Report>