INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

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

For cross certification from MTCS SS to ISO/IEC 27001:2013

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 ISO/IEC 27001:2013 was appointed by IDA to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

Jason Kong	BSI Group Singapore Pte Ltd
Cheng Loon, Dave	Certification International (Singapore) Pte Ltd
Ros Oh	DNV Business Assurance Singapore Pte Ltd
Lee Lai Mei	SGS International Certification Services Singapore Pte Ltd
Indranil Mukherjee	Singapore ISC Pte Ltd
Carol Sim	TÜV Rheinland Singapore Pte Ltd
Chris Ng	TÜV SÜD PSB Pte Ltd

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

Contents

1 Normative References 7

2 Purpose of Document 7

3 Intended Audience 8

4 Document Structure 8

5 Terms and Definitions 9

6 Approach 9

7 Summary of Findings 10

7.1 Summary by Levels in MTCS SS 13

7.2 Summary by Control Areas 15

7.3 Snapshot of Differences between Levels of MTCS SS 18

8 Tips on Using this Gap Analysis Report 20

9 Gap Analysis 21

1 Normative References

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

- **Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS).** MTCS SS aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS SS provides relevant cloud computing security practices and controls for cloud users, auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers to strengthen and demonstrate the cloud security controls in their cloud environments.

- **ISO/IEC 27001:2013** *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.

Documents which provide additional context, including examples and guidance which may or may not have been implemented by the Cloud Service Providers, such as ISO/IEC 27002, are not covered in this report.

2 Purpose of Document

This Gap Analysis Report is the first report in the set of three (3) documents to support cross-certification between MTCS SS 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 ISO/IEC 27001:2013 Standard. The information provided in this document aims to assist entities that are MTCS SS certified to adopt the ISO/IEC 27001:2013 Standard. Cloud Service Providers that are MTCS SS certified will have to comply with the requirements stated in ISO/IEC 27001:2013 Standard 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 the ISO/IEC 27001:2013. 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, ISO/IEC 27001:2013 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 ISO/IEC 27001:2013 certification audit when the scope of MTCS SS audit overlaps with scope of the ISO/IEC 27001:2013 audit.

3 Intended Audience

This Gap Analysis Report is intended for Cloud Service Providers that are MTCS SS Levels 1, 2 or 3 certified who are interested in obtaining ISO/IEC 27001:2013 certification.

This report is also intended to guide auditors, including internal audit function, ISO/IEC 27001:2013 Certification Bodies and external audit bodies on the differences between ISO/IEC 27001:2013 Standard and MTCS SS.

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

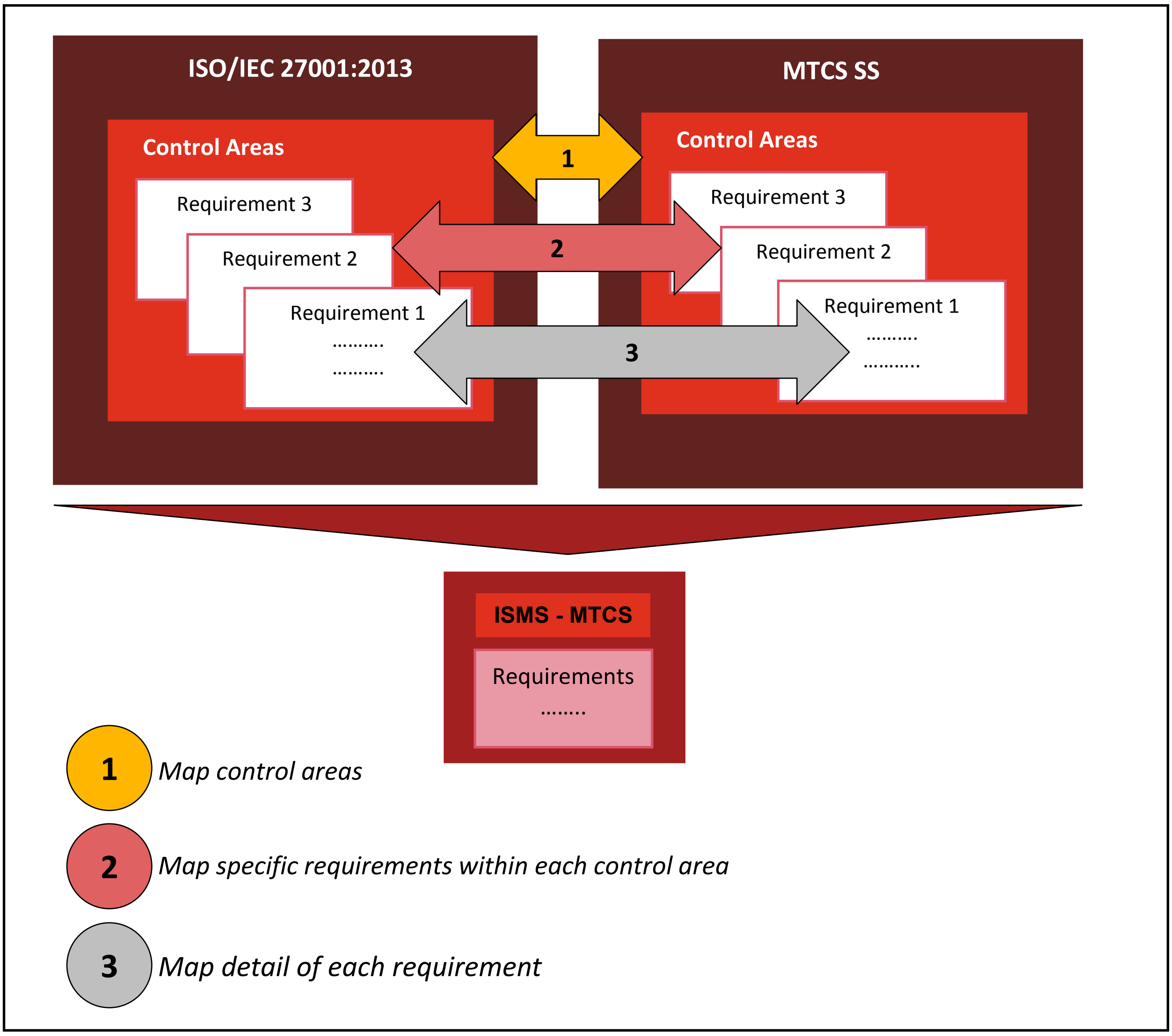
5 Terms and Definitions

ISMS-related terms used in this report are defined in ISO/IEC 27001:2013, and cloud-related terms used in this report are defined in MTCS SS.

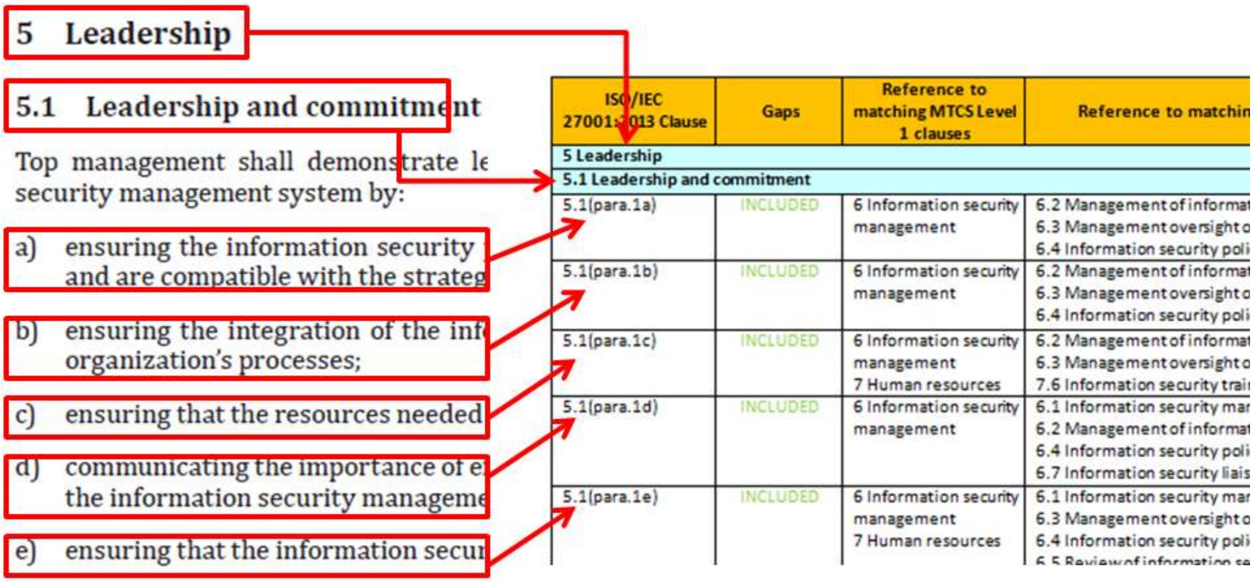
6 Approach

In order to assist Cloud Service Providers that are MTCS SS certified to adopt ISO/IEC 27001:2013, requirements listed in MTCS SS were mapped against equivalent requirements in ISO/IEC 27001:2005. This followed a structured and systematic three (3) step approach:

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



An excerpt of how the actual mapping is done in the document is illustrated below:



5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate le security management system by:

a) ensuring the information security and are compatible with the strateg

b) ensuring the integration of the inf organization's processes;

c) ensuring that the resources needed

d) communicating the importance of e the information security manageme

e) ensuring that the information secur

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS Level 1 clauses	Reference to matchin
5 Leadership			
5.1 Leadership and commitment			
5.1(para.1a)	INCLUDED	6 Information security management	6.2 Management of informat 6.3 Management oversight o 6.4 Information security poli
5.1(para.1b)	INCLUDED	6 Information security management	6.2 Management of informat 6.3 Management oversight o 6.4 Information security poli
5.1(para.1c)	INCLUDED	6 Information security management 7 Human resources	6.2 Management of informat 6.3 Management oversight o 7.6 Information security trai
5.1(para.1d)	INCLUDED	6 Information security management	6.1 Information security mar 6.2 Management of informat 6.4 Information security poli 6.7 Information security liais
5.1(para.1e)	INCLUDED	6 Information security management 7 Human resources	6.1 Information security mar 6.3 Management oversight o 6.4 Information security poli 6.5 Review of information se

7 Summary of Findings

The purpose of this summary section is to provide an overview of the differences between ISO/IEC 27001:2013 and MTCS SS categorised as follows:

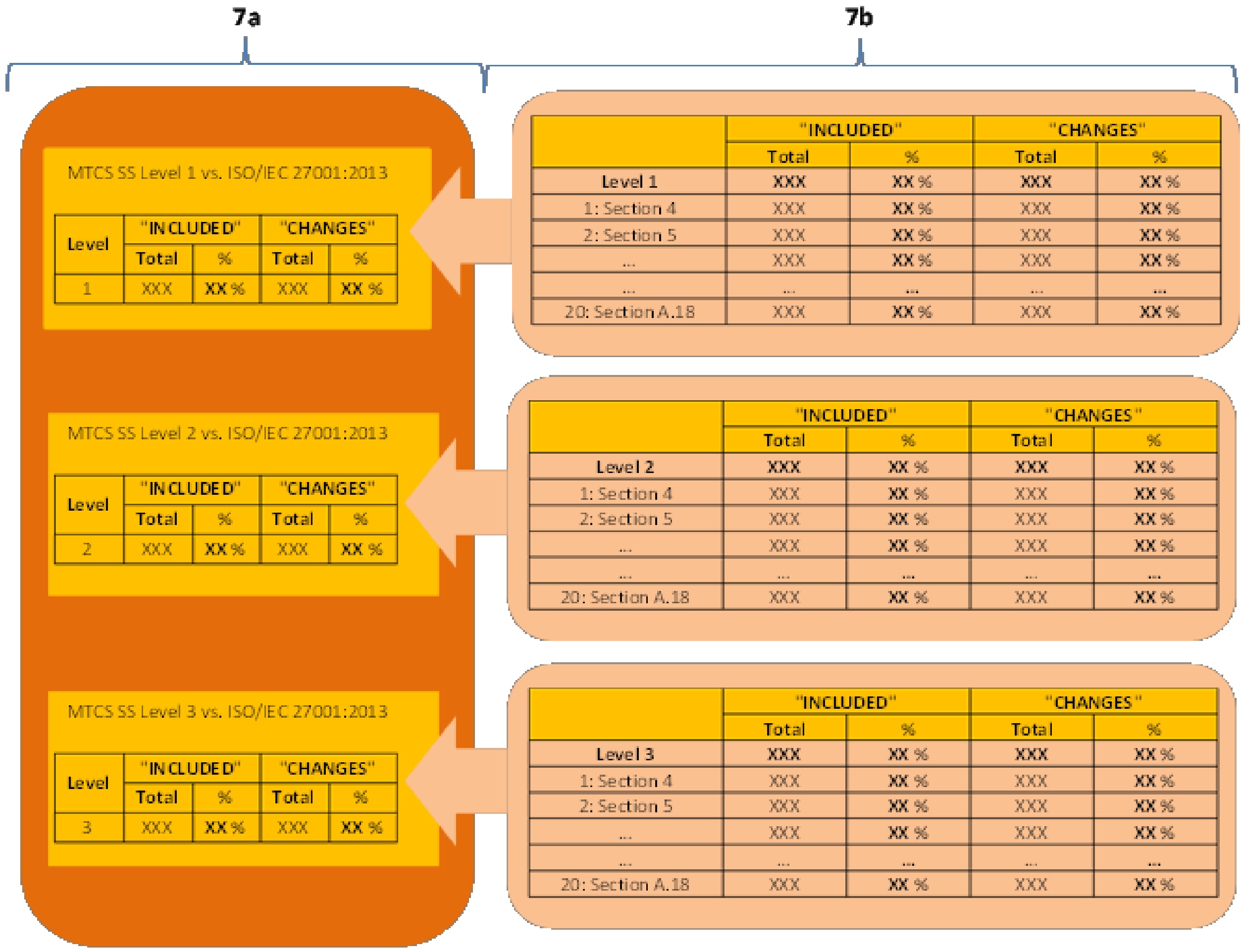
a. Summary by Levels in MTCS SS certification (Levels 1, 2 and 3)

Section 7.1 summarises the total gaps identified for each of the three (3) levels of MTCS SS as compared to the ISO/IEC 27001:2013.

b. Summary by Control Areas 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 twenty-one (21) areas of the ISO/IEC 27001:2013.

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



MTCS SS Level 1 vs. ISO/IEC 27001:2013

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

MTCS SS Level 2 vs. ISO/IEC 27001:2013

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

MTCS SS Level 3 vs. ISO/IEC 27001:2013

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

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 1	XXX	XX %	XXX	XX %
1: Section 4	XXX	XX %	XXX	XX %
2: Section 5	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
20: Section A.18	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 2	XXX	XX %	XXX	XX %
1: Section 4	XXX	XX %	XXX	XX %
2: Section 5	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
20: Section A.18	XXX	XX %	XXX	XX %

	"INCLUDED"		"CHANGES"	
	Total	%	Total	%
Level 3	XXX	XX %	XXX	XX %
1: Section 4	XXX	XX %	XXX	XX %
2: Section 5	XXX	XX %	XXX	XX %
...	XXX	XX %	XXX	XX %
...	...	...	...	...
20: Section A.18	XXX	XX %	XXX	XX %

Cloud Service Providers that are MTCS SS certified and are interested in obtaining ISO/IEC 27001:2013 certification can view the key areas that require enhancements / upgrades in order to adopt the ISO/IEC 27001:2013 Standard. Descriptions of the respective columns are listed below:

Column	Column description
Total Clauses	Indicates the number of clauses that are currently listed in the ISO/IEC 27001:2013.
INCLUDED	Indicates the number of clauses in the ISO/IEC 27001:2013 that are equally represented in the MTCS SS.
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 the ISO/IEC 27001:2013 that are stated with more details than the corresponding sections in clauses in the MTCS SS. 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 the ISO/IEC 27001:2013 that are absent, or stated with significantly more detail than the corresponding sections and clauses in the MTCS SS. In general, the requirements are classified as "NEW" if there may be material financial cost to meet relevant ISO/IEC 27001:2013 requirement, additional controls to be included in the audit checklist and / or the effort is relatively onerous.

The colours green, yellow and red denote the following:

- Green denotes >= 50% ISO/IEC 27001:2013 controls included in MTCS SS.
- Yellow denotes >= 20% and < 50% ISO/IEC 27001:2013 controls included in MTCS SS.
- Red denotes < 20% ISO/IEC 27001:2013 controls included in MTCS SS.

As the MTCS SS is built on recognised international standards such as ISO/IEC 27001:2005, from a high level perspective, the identified gaps primarily cover the differences between ISO/IEC 27001:2005 and ISO/IEC 27001:2013 and ISO/IEC 27001:2013 specific verbiage.

7.1 Summary by Levels in MTCS SS

The purpose of this section by Levels section is to provide an overview of the differences between the ISO/IEC 27001:2013 Standard and MTCS SS as grouped by MTCS SS certification Levels 1, 2 or 3. Cloud Service Providers that are MTCS SS certified and are interested in obtaining ISO/IEC 27001:2013 certification can view the effort required on identified enhancements / upgrades in order to adopt ISO/IEC 27001:2013.

Level 1

The table below provides a high level summary of the differences between ISO/IEC 27001:2013 and MTCS SS Level 1. Cloud Service Providers looking to be cross certified to ISO/IEC 27001:2013 can refer to this table for total requirements applicable to this level[1]:

Total Clauses in ISO/IEC27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
	Total	%	Total	%	Total	%	Total	%
254	220	87%	34	13%	32	13%	2	1%

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

Level 2

The table below provides a high level summary of the differences between ISO/IEC 27001:2013 and MTCS SS Level 2. Cloud Service Providers looking to be cross certified to ISO/IEC 27001:2013 can refer to this table for total requirements applicable to this level[1]:

Total Clauses in ISO/IEC27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
	Total	%	Total	%	Total	%	Total	%
254	228	90%	26	10%	25	10%	1	1%

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

Level 3

The table below provides a high level summary of the differences between ISO/IEC 27001:2013 and MTCS SS Level 3. Cloud Service Providers looking to be cross certified to ISO/IEC 27001:2013 can refer to this table for total requirements applicable to this level[1]:

Total Clauses in ISO/IEC27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
	Total	%	Total	%	Total	%	Total	%
254	230	91%	24	9%	24	9%	0	0%

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

In MTCS SS Level 3, Clause 6.1.4 requires the Cloud Service Provider to be ISO/IEC 27001 certified. Therefore, for any MTCS SS Level 3 certified Cloud Service Provider, there should not be any gaps under the above section. However, MTCS SS is built on ISO/IEC 27001:2005 and the ISO/IEC 27001:2013 Standard was not published at the time of release of the MTCS SS, therefore the identified gaps primarily cover the differences between ISO/IEC 27001:2005 and ISO/IEC 27001:2013.

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 Areas

The purpose of this section is to provide an overview of the differences between the ISO/IEC 27001:2013 Standard and MTCS SS grouped by MTCS SS Levels and the respective control areas in ISO/IEC 27001:2013. Cloud Service Providers that are MTCS SS certified and are interested in obtaining ISO/IEC 27001:2013 certification can view the key logical areas that require enhancements / upgrades in order to adopt ISO/IEC 27001:2013. The table below summarises the differences between MTCS SS Level 1 and ISO/IEC 27001:2013[1]:

Section / Clause No.	Topic	Total Clauses in ISO/IEC 27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
			Total	%	Total	%	Total	%	Total	%
4	Context of the organization	9	9	100%	0	0%	0	0%	0	0%
5	Leadership	18	17	94%	1	6%	1	6%	0	0%
6	Planning	37	29	78%	8	22%	8	22%	0	0%
7	Support	27	22	81%	5	19%	5	19%	0	0%
8	Operation	8	7	88%	1	13%	1	13%	0	0%
9	Performance evaluation	29	16	55%	13	45%	12	41%	1	3%
10	Improvement	12	9	75%	3	25%	3	25%	0	0%
A.5	Information security policies	2	2	100%	0	0%	0	0%	0	0%
A.6	Organization of information security	7	7	100%	0	0%	0	0%	0	0%
A.7	Human resource security	6	6	100%	0	0%	0	0%	0	0%
A.8	Asset management	10	9	90%	1	10%	0	0%	1	10%
A.9	Access control	14	13	93%	1	7%	1	7%	0	0%
A.10	Cryptography	2	2	100%	0	0%	0	0%	0	0%
A.11	Physical and environmental security	15	15	100%	0	0%	0	0%	0	0%
A.12	Operations security	14	14	100%	0	0%	0	0%	0	0%
A.13	Communications security	7	7	100%	0	0%	0	0%	0	0%
A.14	System acquisition, development and maintenance	13	13	100%	0	0%	0	0%	0	0%
A.15	Supplier relationships	5	5	100%	0	0%	0	0%	0	0%
A.16	Information security incident management	7	7	100%	0	0%	0	0%	0	0%
A.17	Information security aspects of business continuity management	4	4	100%	0	0%	0	0%	0	0%
A.18	Compliance	8	7	88%	1	13%	1	13%	0	0%
	TOTAL	**254**	**220**	**87%**	**34**	**13%**	**32**	**13%**	**2**	**1%**

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

The table below summarises the differences between MTCS SS Level 2 and ISO/IEC 27001:2013[1]:

Section / Clause No.	Topic	Total Clauses in ISO/IEC 27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
			Total	%	Total	%	Total	%	Total	%
4	Context of the organization	9	9	100%	0	0%	0	0%	0	0%
5	Leadership	18	17	94%	1	6%	1	6%	0	0%
6	Planning	37	33	89%	4	11%	4	11%	0	0%
7	Support	27	23	85%	4	15%	4	15%	0	0%
8	Operation	8	8	100%	0	0%	0	0%	0	0%
9	Performance evaluation	29	16	55%	13	45%	12	41%	1	3%
10	Improvement	12	9	75%	3	25%	3	25%	0	0%
A.5	Information security policies	2	2	100%	0	0%	0	0%	0	0%
A.6	Organization of information security	7	7	100%	0	0%	0	0%	0	0%
A.7	Human resource security	6	6	100%	0	0%	0	0%	0	0%
A.8	Asset management	10	10	100%	0	0%	0	0%	0	0%
A.9	Access control	14	13	93%	1	7%	1	7%	0	0%
A.10	Cryptography	2	2	100%	0	0%	0	0%	0	0%
A.11	Physical and environmental security	15	15	100%	0	0%	0	0%	0	0%
A.12	Operations security	14	14	100%	0	0%	0	0%	0	0%
A.13	Communications security	7	7	100%	0	0%	0	0%	0	0%
A.14	System acquisition, development and maintenance	13	13	100%	0	0%	0	0%	0	0%
A.15	Supplier relationships	5	5	100%	0	0%	0	0%	0	0%
A.16	Information security incident management	7	7	100%	0	0%	0	0%	0	0%
A.17	Information security aspects of business continuity management	4	4	100%	0	0%	0	0%	0	0%
A.18	Compliance	8	8	100%	0	0%	0	0%	0	0%
	TOTAL	**254**	**228**	**90%**	**26**	**10%**	**25**	**10%**	**1**	**0%**

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

The table below summarises the differences between MTCS SS Level 3 and ISO/IEC 27001:2013[1]:

Section / Clause No.	Topic	Total Clauses in ISO/IEC 27001:2013	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
			Total	%	Total	%	Total	%	Total	%
4	Context of the organization	9	9	100%	0	0%	0	0%	0	0%
5	Leadership	18	17	94%	1	6%	1	6%	0	0%
6	Planning	37	33	89%	4	11%	4	11%	0	0%
7	Support	27	24	89%	3	11%	3	11%	0	0%
8	Operation	8	8	100%	0	0%	0	0%	0	0%
9	Performance evaluation	29	16	55%	13	45%	13	45%	0	0%
10	Improvement	12	10	83%	2	17%	2	17%	0	0%
A.5	Information security policies	2	2	100%	0	0%	0	0%	0	0%
A.6	Organization of information security	7	7	100%	0	0%	0	0%	0	0%
A.7	Human resource security	6	6	100%	0	0%	0	0%	0	0%
A.8	Asset management	10	10	100%	0	0%	0	0%	0	0%
A.9	Access control	14	13	93%	1	7%	1	7%	0	0%
A.10	Cryptography	2	2	100%	0	0%	0	0%	0	0%
A.11	Physical and environmental security	15	15	100%	0	0%	0	0%	0	0%
A.12	Operations security	14	14	100%	0	0%	0	0%	0	0%
A.13	Communications security	7	7	100%	0	0%	0	0%	0	0%
A.14	System acquisition, development and maintenance	13	13	100%	0	0%	0	0%	0	0%
A.15	Supplier relationships	5	5	100%	0	0%	0	0%	0	0%
A.16	Information security incident management	7	7	100%	0	0%	0	0%	0	0%
A.17	Information security aspects of business continuity management	4	4	100%	0	0%	0	0%	0	0%
A.18	Compliance	8	8	100%	0	0%	0	0%	0	0%
	TOTAL	**254**	**230**	**91%**	**24**	**9%**	**24**	**9%**	**0**	**0%**

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

7.3 Snapshot of Differences between Levels of MTCS SS

Of the identified gaps, 24 are common for all 3 levels, the table below summarises the 24 common gaps identified:

ISO/IEC 27001:2013 Topic	ISO/IEC 27001:2013 Sub-topic	No	ISO/IEC 27001:2013 Clause
Leadership	Policy	1	5.2(para.1b)
Planning	Actions to address risks and opportunities	2	6.1.2(para.1b)
		3	6.1.2(para.1c2)
		4	6.1.3(para.1f)
	Information security objectives and planning to achieve them	5	6.2(para.1)
Support	Competence	6	7.2(para.1c)
		7	7.2(para.1d)
	Documented information	8	7.5.2(para.1b)
Performance evaluation	Internal audit	9	9.2(para.1a2)
		10	9.2(para.2f)
	Management review	11	9.3(para.2a)
		12	9.3(para.2b)
		13	9.3(para.2c1)
		14	9.3(para.2c2)
		15	9.3(para.2c3)
		16	9.3(para.2c4)
		17	9.3(para.2d)
		18	9.3(para.2e)
		19	9.3(para.2f)
		20	9.3(para.3)
		21	9.3(para.4)
Improvement	Nonconformity and corrective action	22	10.1(para.3f)
		23	10.1(para.3g)
Access Control	System and application access control	24	A.9.4.1

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

ISO/IEC 27001:2013 Topic	ISO/IEC 27001:2013 Sub-topic	No	ISO/IEC 27001:2013 Clause
Planning	Actions to address risks and opportunities	1	6.1.2(para.1e1)
		2	6.1.2(para.1e2)
	Information security objectives and planning to achieve them	3	6.2(para.2b)
		4	6.2(para.2c)
Support	Documented Information	5	7.5.3(para.2f)
Operation	Information security risk treatment	6	8.3(para.2)
Asset management	Information classification	7	A.8.2.1
Compliance	Compliance with legal and contractual requirements	8	A.18.1.4

[1]These are relevant for MTCS SS Level 1

Cloud Service Providers certified to MTCS SS Level 3 may disregard the following:

ISO/IEC 27001:2013 Topic	ISO/IEC 27001:2013 Sub-topic	No	ISO/IEC 27001:2013 Clause
Support	Documented information	1	7.5.3(para.2d)
Improvement	Nonconformity and corrective action	2	10.1(para.1d)

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 "ISO/IEC 27001:2013 Clause" lists down the clauses that are currently stated in the ISO/IEC 27001:2013 Standard. Relevant clause numbers are appended with references to paragraphs and alphabetical subpoints within the respective clauses.

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 sections” specifies the sections that are currently stated in the MTCS SS and have equal requirements or components relevant to the corresponding ISO/IEC 27001:2013 clause specified under the column “ISO/IEC 27001:2013 Clause”.

4) The column “Reference to matching MTCS sub-sections” specifies the sub-sections that are currently stated in the MTCS SS and have equal requirements or components relevant to the corresponding ISO/IEC 27001:2013 clause specified under the column “ISO/IEC 27001:2013 Clause”. The corresponding parent sections of these sub-sections can be found under the column “Reference to matching MTCS sections”.

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

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 ISO/IEC 27001:2013 document 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. Refer to 4.3 in ISO/IEC27001:2013.

9 Gap Analysis

The purpose of this section is to list the differences between the ISO/IEC 27001:2013 Standard and MTCS SS describing gaps discovered in each control area and their respective clauses.

The table below summarises the list of requirements in ISO/IEC27001:2013 and the respective classification of gaps in relation to MTCS SS Levels 1, 2 and 3 requirements.

Where level is not specified (e.g., 4.1(para.1)) under the column "Gaps", the gap applies to all MTCS SS Levels. Refer to 6.2(para.1e1) for a scenario where there are differences in gaps across the 3 levels.

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
4 Context of the organization				
4.1 Understanding the organization and its context				
4.1(para.1)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	Based on the assumption that Cloud Service Providers have determined external and internal issues that are relevant to ISMS (both cloud-specific and traditional requirements).
4.2 Understanding the needs and expectations of interested parties				
4.2(para.1a)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	Based on the assumption that Cloud Service Providers have determined the interested parties (both internal and external) that are relevant to ISMS (both cloud-specific and traditional requirements).
4.2(para.1b)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	
4.3 Determining the scope of the information security management system				
4.3(para.1)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	Based on the assumption that Cloud Service Providers have determined the boundaries and applicability of the ISMS (both cloud-specific and traditional requirements).

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
4.3(para.2a)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	Based on the assumption that Cloud Service Providers have considered the external and internal issues referred to in ISO/IEC 27001:2013 Clause 4.1 while determining the boundaries and applicability of the ISMS (both cloud-specific and traditional requirements).
4.3(para.2b)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	Based on the assumption that Cloud Service Providers have considered the requirements referred to in ISO/IEC 27001:2013 Clause 4.2 while determining the boundaries and applicability of the ISMS (both cloud-specific and traditional requirements).
4.3(para.2c)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	Based on the assumption that Cloud Service Providers have considered the interfaces and dependencies between activities performed by the organisation, and those performed by other organisations, while determining the boundaries and applicability of the ISMS (both cloud-specific and traditional requirements).
4.3(para.3)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	While documentation of scope is not explicitly mentioned, a scope statement or scope-related information is typically included within information security policies and relevant plans/procedures.
4.4 Information security management system				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
4.4(para.1)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	N.A
5 Leadership				
5.1 Leadership and commitment				
5.1(para.1a)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.1(para.1b)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.1(para.1c)	INCLUDED	6 Information security management	6.2 Management of information security	N.A
5.1(para.1d)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
5.1(para.1e)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
5.1(para.1f)	INCLUDED	6 Information security management	6.2 Management of information security 6.4 Information security policy	N.A
5.1(para.1g)	INCLUDED	6 Information security management	6.2 Management of information security 6.3 Management oversight of information security 6.4 Information security policy 6.5 Review of information security policy	N.A
5.1(para.1h)	INCLUDED	6 Information security management	6.2 Management of information security 6.3 Management oversight of information security	N.A
5.2 Policy				
5.2(para.1a)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.2(para.1b)	INCREMENTAL	6 Information security management	6.4 Information security policy	While an information security policy (MTCS SS Clause 6.4) is able to establish the direction of the organisation, the inclusion of information security objectives in the information security policy is not explicitly mentioned.

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
5.2(para.1c)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.2(para.1d)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.2(para.2e)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.2(para.2f)	INCLUDED	6 Information security management	6.4 Information security policy	N.A
5.2(para.2g)	INCLUDED	6 Information security management	6.4 Information security policy	Communicating the policy to relevant parties would imply making it available as needed.
5.3 Organizational roles, responsibilities and authorities				
5.3(para.1)	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 6.4 Information security policy	N.A
5.3(para.2a)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
5.3(para.2b)	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 6.4 Information security policy	N.A
6 Planning				
6.1 Actions to address risks and opportunities				
6.1.1 General				
6.1.1(para.1)	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 6.4 Information security policy 6.5 Review of information security policy	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
6.1.1(para.1a)	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 6.4 Information security policy 6.5 Review of information security policy	N.A
6.1.1(para.1b)	INCLUDED	6 Information security management 8 Risk management	6.1 Information security management system (ISMS) 6.2 Management of information security 6.3 Management oversight of information security 6.4 Information security policy 8.1 Risk management program	N.A
6.1.1(para.1c)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
6.1.1(para.2d)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
6.1.1(para.2e1)	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 6.4 Information security policy	N.A
6.1.1(para.2e2)	INCLUDED	6 Information security management	6.1 Information Security Management System	N.A
6.1.2 Information security risk assessment				
6.1.2(para.1a1)	INCLUDED	8 Risk management	8.1 Risk management program	N.A
6.1.2(para.1a2)	INCLUDED	8 Risk management	8.2 Risk assessment	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
6.1.2(para.1b)	INCREMENTAL	8 Risk management	8.1 Risk management program 8.2 Risk assessment	While ensuring periodic risk assessments produce consistent, valid and comparable results is not mentioned, inclusion of specific types of risks (MTCS SS Clause 8.2.2(c)) in assessments, and associated documentation can assist in the production of consistent, valid and comparable results. Above gap is not stated clearly as whether it is still a gap if MTCS SS Clause 8.2.2(c) is met.
6.1.2(para.1c1)	INCLUDED	8 Risk management	8.1 Risk management program 8.2 Risk assessment	N.A
6.1.2(para.1c2)	INCREMENTAL	8 Risk management	8.1 Risk management program	While identification of risks (MTCS SS Clause 8.1) can be observed, the identification of risk owners is not specifically mentioned.
6.1.2(para.1d1)	INCLUDED	8 Risk management	8.2 Risk assessment	N.A
6.1.2(para.1d2)	INCLUDED	8 Risk management	8.2 Risk assessment	N.A
6.1.2(para.1d3)	INCLUDED	8 Risk management	8.1 Risk management program 8.2 Risk assessment 8.3 Risk Management 8.4 Risk Register	N.A
6.1.2(para.1e1)	LEVEL 1: INCREMENTAL LEVEL 2: INCLUDED LEVEL 3: INCLUDED	8 Risk management	8.1 Risk management program 8.2 Risk assessment 8.3 Risk Management 8.4 Risk Register	While MTCS SS Level 1 covers risk assessments (MTCS SS Clauses 8.1 and 8.2), risk criteria is only specifically mentioned in Level 2 of MTCS SS Clauses 8.1 and 8.4.
6.1.2(para.1e2)	LEVEL 1: INCREMENTAL LEVEL 2: INCLUDED	8 Risk management	8.1 Risk management program 8.2 Risk assessment 8.3 Risk Management	While MTCS SS Level 1 covers risk assessments (MTCS SS Clauses 8.1 and 8.2), risk prioritisation is only

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
	LEVEL 3: INCLUDED		8.4 Risk Register	specifically mentioned in Level 2 of MTCS SS Clauses 8.1, 8.3 and 8.4.
6.1.2(para.2)	INCLUDED	8 Risk management	8.1 Risk management program	N.A
6.1.3 Information security risk treatment				
6.1.3(para.1a)	INCLUDED	8 Risk management	8.1 Risk management program 8.3 Risk Management 8.4 Risk Register	N.A
6.1.3(para.1b)	INCLUDED	8 Risk management	8.1 Risk management program 8.3 Risk Management 8.4 Risk Register	N.A
6.1.3(para.1c)	INCLUDED	All sections in the MTCS SS (Section 6 to Section 24)	All sections in the MTCS SS (Section 6 to Section 24)	See individual controls from Annex A in this document for details.
6.1.3(para.1d)	INCLUDED	N.A	N.A	Statement of Applicability (SoA) is equivalent to the audit results of the MTCS SS reviews defined under 'Audit Procedures' for each sub-section.
6.1.3(para.1e)	INCLUDED	8 Risk management	8.1 Risk management program 8.3 Risk Management 8.4 Risk Register	N.A
6.1.3(para.1f)	INCREMENTAL	8 Risk management	8.1 Risk management program 8.4 Risk register	Risk owner's approval of the information security risk treatment plan and acceptance of the residual information security risks are not formally mentioned.
6.1.3(para.2)	INCLUDED	8 Risk management	8.1 Risk management program 8.3 Risk Management 8.4 Risk Register	N.A
6.2 Information security objectives and planning to achieve them				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
6.2(para.1)	INCREMENTAL	6 Information security management	6.4 Information security policy	MTCS SS does not specifically cover security objectives including the establishment of information security objectives at relevant functions and levels.
6.2(para.2a)	INCLUDED	6 Information security management	6.4 Information security policy	An information security policy that establishes the direction of the organization and is aligned with industry accepted practices, regulatory and international laws, and is supported by a strategic plan and a security program would imply consistency with security objectives.
6.2(para.2b)	LEVEL 1: INCREMENTAL	6 Information security management	6.1 Information security management system (ISMS) 6.5 Review of information security policy	Development of metrics to measure information security objectives is not mentioned in MTCS SS Level 1. To be able to determine the effectiveness of the policy (MTCS SS Clause 6.5) would imply some elements of measurements. Thus, it would require defining some quantitative or qualitative parameters that can assist in measuring the effectiveness and fulfilling the objective of ISO/IEC 27001:2013 control 6.2(para.2b).
	LEVEL 2: INCLUDED			To be able to determine if the ISMS is functioning properly (MTCS SS Level 2 Clause 6.1) would imply elements of measurements for the whole of ISMS in general, including development of metrics to measure information

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
	LEVEL3: INCLUDED			security objectives. Thus, it would require defining some quantitative or qualitative parameters that can assist in measuring the effectiveness and fulfilling the objective of ISO/IEC 27001:2013 control 6.2(para.2b).
6.2(para.2c)	LEVEL 1: INCREMENTAL	6 Information security management 8 Risk management	6.4 Information security policy 6.5 Review of information security policy 8.3 Risk management	While there are no explicit mentions of taking into account applicable information security requirements, and results from risk assessment and risk treatment in the development of information security objectives, elements of them can be observed from the organisation's approach to managing information security (MTCS SS Clause 6.4), and review and update of the information security policy (MTCS SS Clause 6.5).In addition, checking against results of risk assessment is only specifically mentioned in MTCS SS Level 2 Clause 8.3.
	Level 2: INCLUDED			
	Level 3: INCLUDED			
6.2(para.2d)	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
6.2(para.2e)	INCLUDED	6 Information security management	6.5 Review of information security policy 6.7 Information security liaisons (ISL)	N.A
6.2(para.3)	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
6.2(para.4f)	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 6.4 Information security policy	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
6.2(para.4g)	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 6.4 Information security policy	N.A
6.2(para.4h)	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 6.4 Information security policy	N.A
6.2(para.4i)	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 6.4 Information security policy	N.A
6.2(para.4j)	INCLUDED	6 Information security management	6.3 Management oversight of information security 6.6 Information security audits	N.A
7 Support				
7.1 Resources				
7.1(para.1)	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
7.2 Competence				
7.2(para.1a)	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
7.2(para.1b)	INCLUDED	6 Information security management 7 Human resources	6.2 Management of information security 7.1 Background screening 7.2Continuous personnel evaluation	N.A
7.2(para.1c)	INCREMENTAL	6 Information security management	6.1 Information security management system (ISMS) 6.2 Management of information security	The need for developing competence and thereafter implementing controls to measure its effectiveness is not specifically mentioned in the MTCS SS.

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
7.2(para.1d)	INCREMENTAL	7 Human resources	7 Human resources (all)	The need for the appropriate documentation of the competency of person(s) doing work affecting the organisation's information security performance is not specifically mentioned in the MTCS SS.
7.3 Awareness				
7.3(para.1a)	INCLUDED	6 Information security management 7 Human resources	6.4 Information security policy 7.6 Information security training and awareness	N.A
7.3(para.1b)	INCLUDED	6 Information security management 7 Human resources	6.2 Management of information security 6.4 Information security policy 7.6 Information security training and awareness	While there is no explicit mention of informing people of their contribution to the effectiveness of the ISMS, commitment and direction from the management, however training and awareness programs can include such information and can help to address the control.
7.3(para.1c)	INCLUDED	6 Information security management 7 Human resources	6.2 Management of information security 6.4 Information security policy 7.4 Disciplinary process 7.6 Information security training and awareness	N.A
7.4 Communication				
7.4(para.1)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.4 Information security policy 6.7 Information security liaisons (ISL)	N.A
7.4(para.1a)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.4 Information security policy 6.7 Information security liaisons (ISL)	N.A
7.4(para.1b)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.4 Information security policy 6.7 Information security liaisons (ISL)	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
7.4(para.1c)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.4 Information security policy 6.7 Information security liaisons (ISL)	N.A
7.4(para.1d)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.4 Information security policy 6.7 Information security liaisons (ISL)	N.A
7.4(para.1e)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.4 Information security policy 6.7 Information security liaisons (ISL)	N.A
7.5 Documented information				
7.5.1 General				
7.5.1(para.1a)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
7.5.1(para.1b)	INCLUDED	6 Information security management	6.1 Information security management system (ISMS)	N.A
7.5.2 Creating and updating				
7.5.2(para.1a)	INCLUDED	6 Information security management 12 Data governance	6.1 Information security management system (ISMS) 12.4 Data labelling / handling	While detailed information to identify and describe data is only specified for audit trails, it can be understood that it is common practice to include proper identification and supporting cover information (e.g., version, data, reference number) in the documented information.
7.5.2(para.1b)	INCREMENTAL	6 Information security management	6.1 Information security management system (ISMS)	There is no mention of specific formats and media that is required to bring consistency and completeness across all the documentation of information in the MTCS SS.
7.5.2(para.1c)	INCLUDED	6 Information security management 12 Data governance	6.4 Information security policy 6.5 Review of information security policy 12.4 Data labelling / handling	N.A
7.5.3 Control of documented information				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
7.5.3(para.1)	INCLUDED	12 Data governance	12 Data governance (all)	N.A
7.5.3(para.1a)	INCLUDED	12 Data governance	12 Data governance (all)	N.A
7.5.3(para.1b)	INCLUDED	12 Data governance	12 Data governance (all)	N.A
7.5.3(para.2c)	INCLUDED	6 Information security management 12 Data governance	6.1 Information security management system (ISMS) 12.5 Data Protection	N.A
7.5.3(para.2d)	LEVEL1: INCREMENTAL LEVEL2: INCREMENTAL LEVEL 3: INCLUDED	6 Information security management 12 Data governance	6.1 Information security management system (ISMS) 12.5 Data protection 12.6 Data retention	While there are elements of storage and data protection in MTCS SS, details of storage protection, redundancy and testing are not mentioned in sufficient details except in Level 3 of MTCS SS Clauses 12.5 and 12.6.
7.5.3(para.2e)	INCLUDED	12 Data governance 20 Change management	12.4 Data labelling / handling 20.1 Change management process	N.A
7.5.3(para.2f)	LEVEL1: INCREMENTAL LEVEL 2: INCLUDED LEVEL 3: INCLUDED	12 Data governance	12.6 Data retention 12.8 Secure disposal and decommissioning of hardcopy, media and equipment 12.9 Secure disposal verification of live instances and backup	Retention is not explicitly mentioned except in Levels 2 and 3 of MTCS SS Clause 12.6.
7.5.3(para.3)	INCLUDED	12 Data governance	12.4 Data labelling / handling 12.5 Data protection 12.6 Data retention	N.A
8 Operation				
8.1 Operational planning and control				
8.1(para.1)	INCLUDED	19 Operations	19.1 Operations management policies and procedures	N.A
8.1(para.2)	INCLUDED	19 Operations	19.2 Documentation of service operations and external dependencies	N.A
8.1(para.3)	INCLUDED	20 Change management	20.1 Change management process	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
8.1(para.4)	INCLUDED	9 Third party 10 Legal and compliance	9.2 Identification of risks related to third parties 9.3 Third party agreement 9.4 Third party delivery management 10.5 Third party compliance	N.A
8.2 Information security risk assessment				
8.2(para.1)	INCLUDED	8 Risk management	8.1 Risk management program 8.2 Risk assessment	N.A
8.2(para.2)	INCLUDED	8 Risk management	8.1 Risk management program 8.2 Risk assessment 8.3 Risk management	MTCS SS Clause 8.3.3 implies that results of risk assessment have already been documented although there was no explicit mention of the need to document risk assessment results.
8.3 Information security risk treatment				
8.3(para.1)	INCLUDED	8 Risk management	8.1 Risk management program 8.3 Risk management	N.A
8.3(para.2)	LEVEL 1: INCREMENTAL	6 Information security management	6.3 Management oversight of information security	Documentation is mentioned broadly in MTCS SS Clauses 6.1 and 6.3. However, there is no explicit mention about the documentation of the results from information security risk treatment in the MTCS SS until Level 2 of MTCS SS Clause 8.4.
	LEVEL 2: INCLUDED	8 Risk management	8.4 Risk register	
	LEVEL 3: INCLUDED			
9 Performance evaluation				
9.1 Monitoring, measurement, analysis and evaluation				
9.1(para.1)	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
9.1(para.2a)	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 6.4 Information security policy	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
9.1(para.2b)	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 6.4 Information security policy	N.A
9.1(para.2c)	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 6.4 Information security policy	N.A
9.1(para.2d)	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
9.1(para.2e)	INCLUDED	6 Information security management	6.5 Review of information security policy	N.A
9.1(para.2f)	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
9.1(para.3)	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
9.2 Internal audit				
9.2(para.1)	INCLUDED	6 Information security management	6.6 Information security audits	N.A
9.2(para.1a1)	INCLUDED	6 Information security management	6.6 Information security audits	N.A
9.2(para.1a2)	LEVEL 1: NEW	N.A	N.A	Scope of audit committee does not specifically include ISO/IEC 27001:2013 for MTCS SS Levels 1 and 2.
	LEVEL 2: NEW			
	LEVEL 3: INCREMENTAL		6.1 Information security management systems (ISMS)	In MTCS SS Level 3 Clause 6.1.4, MTCS SS requires Cloud Service Providers to have a valid ISO 27001 certification but ISO/IEC 27001:2013 was not published at the time of release of the MTCS SS.

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
9.2(para.1b)	INCLUDED	6 Information security management	6.6 Information security audits	N.A
9.2(para.2c)	INCLUDED	6 Information security management	6.6 Information security audits	N.A
9.2(para.2d)	INCLUDED	6 Information security management	6.6 Information security audits	N.A
9.2(para.2e)	INCLUDED	6 Information security management 10 Legal and compliance	6.6 Information security audits 10.2 Compliance with policies and standards	N.A
9.2(para.2f)	INCREMENTAL	6 Information security management	6.6 Information security audits	There is no explicit mention of reporting audit results to relevant management though the establishment of an audit committee and the identification of participants involved in the meeting or committee, their respective job functions and the reporting relationship (MTCS SS Clause 6.6) could imply so.
9.2(para.2g)	INCLUDED	6 Information security management	6.6 Information security audits	While there is explicit mention of the documentation of audit programme(s) and the audit results, inspection of audit plans and audit reports (MTCS SS Clause 6.6) would imply the existence of documentation.
9.3 Management review				
9.3(para.1)	INCLUDED	6 Information security management	6.2 Management of information security 6.3 Management oversight of information security	N.A
9.3(para.2a)	INCREMENTAL	6 Information security management	6.2 Management of information security 6.3 Management oversight of information security	While there are elements of management reviews (MTCS SS Clauses 6.2 and 6.3), the inclusion of the following topics relevant to the information security management
9.3(para.2b)				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
9.3(para.2c1)				system in management reviews are not mentioned: • status of actions from previous management reviews; • changes in external and internal issues; • feedback on the information security performance, including trends in: ○ nonconformities and corrective actions; ○ monitoring and measurement results; ○ audit results; ○ fulfillment of information security objectives; • feedback from interested parties; • results of risk assessment and status of risk treatment plan; and • opportunities for continual improvement.
9.3(para.2c2)				
9.3(para.2c3)				
9.3(para.2c4)				
9.3(para.2d)				
9.3(para.2e)				
9.3(para.2f)				
9.3(para.3)	INCREMENTAL	6 Information security management	6.2 Management of information security 6.3 Management oversight of information security	While there are elements of management reviews (MTCS SS Clauses 6.2 and 6.3), outputs of the management review are not mentioned including decisions on opportunities of continual improvement and any needs for changes to the information security management system.

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
9.3(para.4)	INCREMENTAL	6 Information security management	6.2 Management of information security 6.3 Management oversight of information security	Documentation is mentioned broadly in MTCS SS Clauses 6.2 and 6.3. However, the documentation of the results of management reviews on the information security management system is not mentioned.
10 Improvement				
10.1 Nonconformity and corrective action				
10.1(para.1a1)	INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 10.6 Continuous compliance monitoring	N.A
10.1(para.1a2)	INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards	N.A
10.1(para.1b1)	INCLUDED	10 Legal and compliance 11 Incident management	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 10.6 Continuous compliance monitoring 11.4 Problem management	N.A
10.1(para.1b2)	INCLUDED	10 Legal and compliance 11 Incident management	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 10.6 Continuous compliance monitoring 11.4 Problem management	N.A
10.1(para.1b3)	INCLUDED	10 Legal and compliance 11 Incident management	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 10.6 Continuous compliance monitoring 11.4 Problem management	N.A
10.1(para.1c)	INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards 10.6 Continuous compliance monitoring	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
10.1(para.1d)	LEVEL 1: INCREMENTAL	11 Incident management	11.4 Problem management	While the control to measure the effectiveness is explicitly included for Level 3 in MTCS SS, it is not defined for Levels 1 and 2.
	LEVEL 2: INCREMENTAL			
	LEVEL 3: INCLUDED			
10.1(para.1e)	INCLUDED	6 Information security management 10 Legal and compliance	6.5 Review of information security policy 10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards	N.A
10.1(para.2)	INCLUDED	11 Incident management	11.4 Problem management	N.A
10.1(para.3f)	INCREMENTAL	11 Incident management	11.1 Information security incident response plan (IS IRP) and procedures 11.4 Problem Management	MTCS SS does not explicitly mention controls to retain documented evidence for the following: • nonconformities, • details of corrective action; and • results of corrective action.
10.1(para.3g)				
10.2 Continual improvement				
10.2(para.1)	INCLUDED	6 Information security management 10 Legal and compliance	6.1 Information security management system 10.2 Compliance with policies and standards	N.A
A.5 Information security policies				
A.5.1 Management direction for information security				
A.5.1.1	INCLUDED	6 Information security management	6.4 Information security policy 6.5 Review of information security policy	N.A
A.5.1.2	INCLUDED	6 Information security management	6.5 Review of information security policy	N.A
A.6 Organization of information security				
A.6.1 Internal organization				
A.6.1.1	INCLUDED	6 Information security management	6.1 Information security management system (ISMS) 6.2 Management of information security	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.6.1.2	INCLUDED	6 Information security management 22 Cloud services administration	6.1 Information security management system (ISMS) 6.2 Management of information security 22.10 Segregation of duties	N.A
A.6.1.3	INCLUDED	6 Information security management	6.7 Information security liaisons (ISL)	N.A
A.6.1.4	INCLUDED	6 Information security management	6.7 Information security liaisons (ISL)	N.A
A.6.1.5	INCLUDED	16System acquisitions and development 20 Change management	16.1 Development, acquisition and release management 20.1 Change management process	While project management is not explicitly mentioned, elements from MTCS SS Clauses 16.1 and 20.1 are components of project management.
A.6.2 Mobile devices and teleworking				
A.6.2.1	INCLUDED	6 Information security management	6.8 Acceptable usage	N.A
A.6.2.2	INCLUDED	6 Information security management	6.8 Acceptable usage	N.A
A.7 Human resource security				
A.7.1 Prior to employment				
A.7.1.1	INCLUDED	7 Human resources	7.1 Background screening	N.A
A.7.1.2	INCLUDED	7 Human resources	7.3 Employment and contract terms and conditions	N.A
A.7.2 During employment				
A.7.2.1	INCLUDED	7 Human resources	7.3 Employment and contract terms and conditions	N.A
A.7.2.2	INCLUDED	7 Human resources	7.6 Information security training and awareness	N.A
A.7.2.3	INCLUDED	7 Human resources	7.4 Disciplinary process	N.A
A.7.3 Termination and change of employment				
A.7.3.1	INCLUDED	7 Human resources	7.3 Employment and contract terms and conditions	N.A
A.8 Asset management				
A.8.1 Responsibility for assets				
A.8.1.1	INCLUDED	18 Physical and environmental	18.1 Asset management	N.A
A.8.1.2	INCLUDED	18 Physical and environmental	18.1 Asset management	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.8.1.3	INCLUDED	6 Information security management	6.8 Acceptable usage	N.A
A.8.1.4	INCLUDED	7 Human resources	7.3 Employment and contract terms and conditions 7.5 Asset returns	N.A
A.8.2 Information classification				
A.8.2.1	LEVEL 1: NEW	N.A	N.A	Classification of information is not mentioned in Level 1 of Clause 12.1 in MTCS SS.
	LEVEL 2: INCLUDED	12 Data governance	12.1 Data classification	N.A
	LEVEL 3: INCLUDED			
A.8.2.2	INCLUDED	6 Information security management 12 Data governance	6.8 Acceptable usage 12.4 Data labelling / handling	N.A
A.8.2.3	INCLUDED	6 Information security management 12 Data governance	6.1 Information security management system (ISMS) 12.4 Data labelling / handling	N.A
A.8.3 Media handling				
A.8.3.1	INCLUDED	12 Data governance	12.4 Data labelling / handling	N.A
A.8.3.2	INCLUDED	12 Data governance	12.8 Secure disposal and decommissioning of hardcopy, media and equipment	N.A
A.8.3.3	INCLUDED	12 Data governance	12.4 Data labelling / handling 12.5 Data protection 12.10 Tracking of data	N.A
A.9 Access control				
A.9.1 Business requirements of access control				
A.9.1.1	INCLUDED	22 Cloud services administration 23 Cloud user access	22.1 Privilege account creation 23.1 User access registration	N.A
A.9.1.2	INCLUDED	22 Cloud services administration 23 Cloud user access	22.1 Privilege account creation 23.1 User access registration 23.2 User access security	N.A
A.9.2 User access management				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.9.2.1	INCLUDED	22 Cloud services administration 23 Cloud user access	22.1 Privilege account creation 23.1 User access registration 23.2 User access security	N.A
A.9.2.2	INCLUDED	22 Cloud services administration 23 Cloud user access	22.1 Privilege account creation 22.3 Administrator access review and revocation 23.1 User access registration 23.2 User access security	N.A
A.9.2.3	INCLUDED	22 Cloud services administration	22.1 Privilege account creation	N.A
A.9.2.4	INCLUDED	16System acquisitions and development 17 Encryption 22 Cloud services administration 23 Cloud user access	16.1 Development, acquisition and release management 17.1 Encryption policies and procedures 22.2 Generation of administrator passwords 22.5 Password change 22.6 Password reset and first logon 22.11 Secure transmission of access credentials 23.3 User access password 23.5 User password reset and 1st logon change 23.6 Password protection	While secret authentication information is not explicitly defined, it can be understood to be sensitive authentication data such as a password or encryption keys.
A.9.2.5	INCLUDED	22 Cloud services administration	22.3 Administrator access review and revocation 22.10 Segregation of duties	N.A
A.9.2.6	INCLUDED	7 Human resources 22 Cloud services administration	7.5 Asset returns 22.3 Administrator access review and revocation	N.A
A.9.3 User responsibilities				
A.9.3.1	INCLUDED	17 Encryption 22 Cloud services administration 23 Cloud user access	17.1 Encryption policies and procedures 17.3 Key management 22.2 Generation of administrator passwords 22.5 Password change 23.3 User access password 23.9 Self-service portal creation and management of user accounts	While secret authentication information is not explicitly defined, it can be understood to be sensitive authentication data such as a password or encryption keys.
A.9.4 System and application access control				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.9.4.1	INCREMENTAL	23 Cloud user access	23.1 User access registration 23.2 User access security	While there are elements of access related controls in MTCS SS, specific requirement related to access control policy is not mentioned.
A.9.4.2	INCLUDED	22 Cloud services administration 23 Cloud user access	22.11 Secure transmission of access credentials 23.1 User access registration 23.2 User access security	N.A
A.9.4.3	INCLUDED	22 Cloud services administration 23 Cloud user access	22.2 Generation of administrator passwords 23.3 User access password 23.5 User password reset and 1st logon change	N.A
A.9.4.4	INCLUDED	14 Secure configuration	14.5 Restrictions to system utilities	N.A
A.9.4.5	INCLUDED	16 System acquisitions and development	16.4 Source code security	N.A
A.10 Cryptography				
A.10.1 Cryptographic controls				
A.10.1.1	INCLUDED	17 Encryption	17.1 Encryption policies and procedures	N.A
A.10.1.2	INCLUDED	17 Encryption	17.3 Key management	N.A
A.11 Physical and environmental security				
A.11.1 Secure areas				
A.11.1.1	INCLUDED	18 Physical and environmental	18.3 Physical access 18.4 Visitors	N.A
A.11.1.2	INCLUDED	18 Physical and environmental	18.3 Physical access 18.4 Visitors	N.A
A.11.1.3	INCLUDED	18 Physical and environmental	18.3 Physical access 18.4 Visitors	N.A
A.11.1.4	INCLUDED	18 Physical and environmental	18.5 Environmental threats and equipment power failures	N.A
A.11.1.5	INCLUDED	18 Physical and environmental	18.3 Physical access	N.A
A.11.1.6	INCLUDED	18 Physical and environmental	18.3 Physical access	N.A
A.11.2 Equipment				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.11.2.1	INCLUDED	18 Physical and environmental	18.1 Asset management 18.5 Environmental threats and equipment power failures	N.A
A.11.2.2	INCLUDED	18 Physical and environmental	18.5 Environmental threats and equipment power failures	N.A
A.11.2.3	INCLUDED	18 Physical and environmental	18.5 Environmental threats and equipment power failures	N.A
A.11.2.4	INCLUDED	18 Physical and environmental	18.1 Asset management	N.A
A.11.2.5	INCLUDED	18 Physical and environmental	18.2 Off-site movement	N.A
A.11.2.6	INCLUDED	9 Third party 18 Physical and environmental	9.2 Identification of risks related to third parties 9.3 Third party agreement 9.4 Third party delivery management 18.1 Asset management	While there is no explicit mention of security of equipment and assets off-premises, it can possibly be addressed under MTCS SS Clauses 9.2, 9.3, 9.4 and 18.1.
A.11.2.7	INCLUDED	12 Data governance	12.8 Secure disposal and decommissioning of hardcopy, media and equipment	N.A
A.11.2.8	INCLUDED	18 Physical and environmental	18.1 Asset management	N.A
A.11.2.9	INCLUDED	18 Physical and environmental	18.1 Asset management	N.A
A.12 Operations security				
A.12.1 Operational procedures and responsibilities				
A.12.1.1	INCLUDED	19 Operations	19.1 Operations management policies and procedures	N.A
A.12.1.2	INCLUDED	20 Change management	20.1 Change management process	N.A
A.12.1.3	INCLUDED	19 Operations	19.3 Capacity management	N.A
A.12.1.4	INCLUDED	20 Change management	20.4 Separation of environment	N.A
A.12.2 Protection from malware				
A.12.2.1	INCLUDED	14 Secure configuration	14.2 Malicious code prevention	N.A
A.12.3 Backup				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.12.3.1	INCLUDED	12 Data governance	12.7 Data backups	N.A
A.12.4 Logging and monitoring				
A.12.4.1	INCLUDED	10 Legal and compliance 13 Audit logging and monitoring	13.1 Logging and monitoring process 13.3 Audit trails	N.A
A.12.4.2	INCLUDED	13 Audit logging and monitoring	13.1 Logging and monitoring process 13.3 Audit trails 13.4 Backup and retention of audit trails 13.5 Usage logs	N.A
A.12.4.3	INCLUDED	13 Audit logging and monitoring 22 Cloud services administration	13.1 Logging and monitoring process 13.3 Audit trails 22.8 Administrator access logs	N.A
A.12.4.4	INCLUDED	13 Audit logging and monitoring	13.1 Logging and monitoring process	N.A
A.12.5 Control of operational software				
A.12.5.1	INCLUDED	14 Secure configuration	14.7 Unauthorised software	N.A
A.12.6 Technical vulnerability management				
A.12.6.1	INCLUDED	15 Security testing and monitoring	15.1 Vulnerability scanning 15.2 Penetration testing 15.3 Security monitoring	N.A
A.12.6.2	INCLUDED	14 Secure configuration	14.7 Unauthorised software	N.A
A.12.7 Information systems audit considerations				
A.12.7.1	INCLUDED	6 Information security management	6.6 Information security audits	N.A
A.13 Communications security				
A.13.1 Network security management				
A.13.1.1	INCLUDED	24 Tenancy and customer isolation	24.3 Network protection	N.A
A.13.1.2	INCLUDED	24 Tenancy and customer isolation	24.3 Network protection	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.13.1.3	INCLUDED	24 Tenancy and customer isolation	24.1 Multi tenancy 24.2 Supporting infrastructure segmentation 24.3 Network protection	N.A
A.13.2 Information transfer				
A.13.2.1	INCLUDED	9 Third party 17 Encryption	9.3 Third party agreement 17.2 Channel encryption	N.A
A.13.2.2	INCLUDED	9 Third party 17 Encryption	9.3 Third party agreement 17.2 Channel encryption	N.A
A.13.2.3	INCLUDED	9 Third party 17 Encryption	9.3 Third party agreement 17.2 Channel encryption	N.A
A.13.2.4	INCLUDED	9 Third party	9.3 Third party agreement	N.A
A.14 System acquisition, development and maintenance				
A.14.1 Security requirements of information systems				
A.14.1.1	INCLUDED	16System acquisitions and development	16.1 Development, acquisition and release management	N.A
A.14.1.2	INCLUDED	12 Data governance 17 Encryption	12.3 Data integrity 17.4 Electronic messaging security	N.A
A.14.1.3	INCLUDED	12 Data governance 17 Encryption	12.3 Data integrity 12.4 Data labelling / handling 17.4 Electronic messaging security	N.A
A.14.2 Security in development and support processes				
A.14.2.1	INCLUDED	16 System acquisitions and development	16.1 Development, acquisition and release management	N.A
A.14.2.2	INCLUDED	16 System acquisitions and development 20 Change management	16.1 Development, acquisition and release management 20.1 Change management process	N.A
A.14.2.3	INCLUDED	16 System acquisitions and development 20 Change management	16.1 Development, acquisition and release management 20.1 Change management process	N.A
A.14.2.4	INCLUDED	16 System acquisitions and development	16.1 Development, acquisition and release management	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.14.2.5	INCLUDED	16 System acquisitions and development	16.1 Development, acquisition and release management	N.A
A.14.2.6	INCLUDED	16 System acquisitions and development 20 Change management	16.1 Development, acquisition and release management 20.4 Separation of environment	N.A
A.14.2.7	INCLUDED	16 System acquisitions and development	16.5 Outsourced software development	N.A
A.14.2.8	INCLUDED	16 System acquisitions and development	16.1 Development, acquisition and release management 16.3 System testing	MTCS SS Clauses 16.1.2(d) and 16.1.2(l) indirectly indicate the need for testing
A.14.2.9	INCLUDED	16 System acquisitions and development 20 Change management	16.1 Development, acquisition and release management 16.3 System testing 20.1 Change management process	MTCS SS Clauses 16.1.2(d) and 16.1.2(l) indirectly indicate the need for testing
A.14.3 Test data				
A.14.3.1	INCLUDED	12 Data governance 16System acquisitions and development	12.11 Production data 16.3 System testing	N.A
A.15 Supplier relationships				
A.15.1 Information security in supplier relationships				
A.15.1.1	INCLUDED	9 Third party	9.2 Identification of risks related to third parties 9.3 Third party agreement 9.4 Third party delivery management	N.A
A.15.1.2	INCLUDED	9 Third party	9.2 Identification of risks related to third parties 9.3 Third party agreement 9.4 Third party delivery management	N.A
A.15.1.3	INCLUDED	9 Third party	9.2 Identification of risks related to third parties 9.3 Third party agreement 9.4 Third party delivery management	N.A
A.15.2 Supplier service delivery management				
A.15.2.1	INCLUDED	9 Third party	9.4 Third party delivery management	N.A
A.15.2.2	INCLUDED	9 Third party	9.4 Third party delivery management	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.16 Information security incident management				
A.16.1 Management of information security incidents and improvements				
A.16.1.1	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
A.16.1.2	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
A.16.1.3	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
A.16.1.4	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures	N.A
A.16.1.5	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
A.16.1.6	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures 11.2 Information security incident response plan testing and updates	N.A
A.16.1.7	INCLUDED	11 Incident management	11.1 Information security incident response plan and procedures	N.A
A.17 Information security aspects of business continuity management				
A.17.1 Information security continuity				
A.17.1.1	INCLUDED	21 Business continuity planning (BCP) and disaster recovery (DR)	21.1 BCP framework 21.2 BCP and DR plans	N.A

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.17.1.2	INCLUDED	21 Business continuity planning (BCP) and disaster recovery (DR)	21.1 BCP framework 21.2 BCP and DR plans	N.A
A.17.1.3	INCLUDED	21 Business continuity planning (BCP) and disaster recovery (DR)	21.1 BCP framework 21.2 BCP and DR plans 21.3 BCP and DR testing	N.A
A.17.2 Redundancies				
A.17.2.1	INCLUDED	21 Business continuity planning (BCP) and disaster recovery (DR)	21.2 BCP and DR plans	N.A
A.18 Compliance				
A.18.1 Compliance with legal and contractual requirements				
A.18.1.1	INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements	N.A
A.18.1.2	INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements	N.A
A.18.1.3	INCLUDED	6 Information security management 10 Legal and compliance 12 Data governance	6.1 Information security management system (ISMS) 10.1 Compliance with regulatory and contractual requirements 12.5 Data protection	N.A
A.18.1.4	LEVEL 1: INCREMENTAL LEVEL 2: INCLUDED LEVEL 3: INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements	High level compliance to regulatory requirements (MTCS SS Clause 10.1) was mentioned but not specific to the privacy and protection of personally identifiable information. Only in Levels 2 and 3 of MTCS SS Clause 10.1 was data protection specifically mentioned.
A.18.1.5	INCLUDED	10 Legal and compliance 17 Encryption	10.4 Use of compliant cryptography controls 17.1 Encryption policies and procedures	N.A
A.18.2 Information security reviews				

ISO/IEC 27001:2013 Clause	Gaps	Reference to matching MTCS sections	Reference to matching MTCS sub-sections	Remarks on identified gaps
A.18.2.1	INCLUDED	10 Legal and compliance	10.1 Compliance with regulatory and contractual requirements 10.2 Compliance with policies and standards	N.A
A.18.2.2	INCLUDED	10 Legal and compliance	10.2 Compliance with policies and standards	N.A
A.18.2.3	INCLUDED	10 Legal and compliance 15 Security testing and monitoring	10.2 Compliance with policies and standards 15.1 Vulnerability scanning 15.2 Penetration testing	N.A

<End of Gap Analysis Report>