INFOCOMM MEDIA DEVELOPMENT AUTHORITY OF SINGAPORE

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

For cross-certification from ISO/IEC 27001:2013 to MTCS SS 584:2020

Oct 2020

Revision History

Revision Date	Version	Updated by	Description
Oct 2020	Version 1.0	IMDA	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), 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 shall not be responsible or liable for reliance by any person on the information, opinions and / or conclusions contained herein. The Working Group 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 is 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 Cloud Computing Standards Technical Committee under the purview of the IT Standards Committee sets up the Multi-tier Cloud Security (MTCS) Working Group (WG) to assist in the revision of MTCS standard, comprises the following experts who contribute in their *individual capacity*:

		Name
Convenor	:	Dr Kang Meng Chow
Deputy Convenor	:	Mr Lim Soon Chia
Members	:	Dr Anton Ravindran
		Mr Mandar Bale
		Dr Ken Baylor
		Mr Chai Chin Loon
		Mr Chan Meng Fai
		Mr Dave Cheng
		Mr Chetan Sansare
		Mr Chong Jian Yi
		Mr Patrick Choong Wee Meng
		Ms Dhana Lakshmi
		Mr Gajun Ganendran
		Mr Hong Jian Hui
		Mr Lucas Kauffman
		Mr Richard Koh
		Prof Lam Kwok Yan
		Dr Lee Hing Yan
		Ms Lim May Ann
		Mr Loh Chee Keong

Mr Manoj Wadhwa

Mr Mok Boon Poh

Mr Chris Ng Khee Soon

Mr Raju Chellam

Mr Sanjeev Gupta

Mr Andrew Seit

Mr Sim Bak Chor

Mr Suresh Agarwal

Mr Tao Yao Sing

Ms Irene Wang

Mr Wong Onn Chee

Mr Xiang Bin

Mr Zhuang Haojie

The organisations in which the experts of the Working Group are involved are:

AliCloud

Amazon Web Services

Asia Cloud Computing Association

Association of Information Security Professionals

BSI Group Singapore Pte. Ltd.

Certification Partner Global

Cloud Security Alliance APAC

Cyber Security Agency

Ernst & Young CertifyPoint B.V.

Google Cloud

Government Technology Agency

IBM Softlayer Cloud

Infocomm Media Development Authority of Singapore

Microsoft Cloud Services

Salesforce.com

SCS Cloud Chapter

SGTech, Cloud and Data Chapter

Singapore Chinese Chamber of Commerce and Industry

SOCOTEC Certification Singapore

TÜV SÜD PSB Pte Ltd

The Multi-Tiered Cloud Security cross-certification Focus Group on ISO/IEC 27001:2013 to MTCS SS584:2020 was formed within the MTCS WG to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

Chong Jian Yi	SOCOTEC Certification Singapore
Manoj Wadhwa	Ernst & Young CertifyPoint B.V.
Sanjeev Gupta	Certification Partner Global
Chris Ng Khee Soon	TÜV SÜD PSB

Please send questions and feedback to nitsc@imda.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.

- **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 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 to support cross certification between ISO/IEC 27001:2013 and MTCS SS584:2020.

Gap Analysis Report
The purpose of the Gap Analysis Report is to provide an overview of the differences between the requirements listed in MTCS SS584:2020 and the ISO/IEC 27001:2013 Standard. The information provided in this document aims to assist entities that are ISO/IEC 27001:2013 certified to adopt MTCS SS. Cloud Service Providers that are ISO/IEC 27001:2013 certified will have to comply with the requirements stated in MTCS SS that are currently omitted in ISO/IEC 27001:2013.

3 Intended Audience

This Gap Analysis Report is intended for Cloud Service Providers that are ISO/IEC 27001:2013 certified and interested in obtaining MTCS SS certification.

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

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

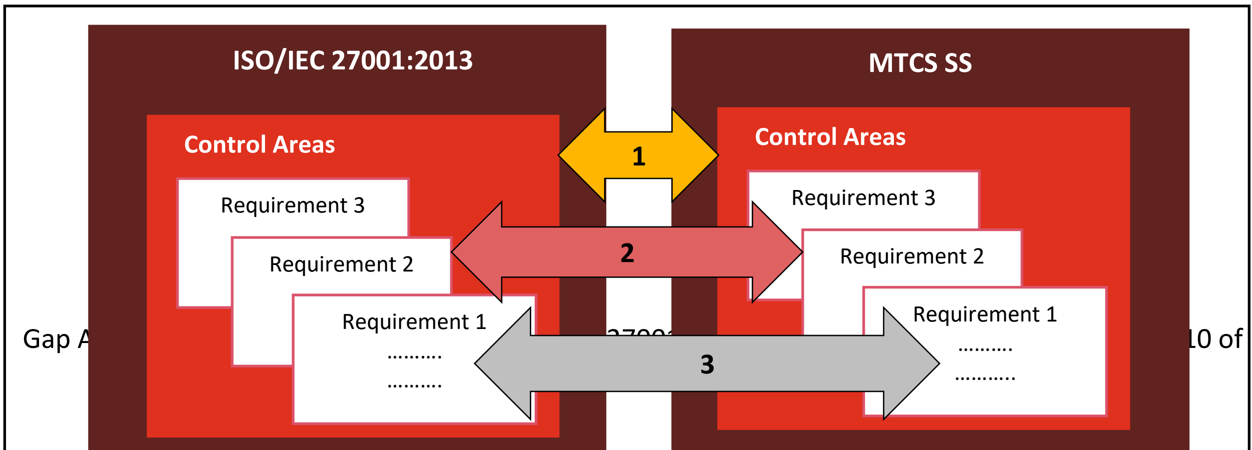
5 Terms and Definitions

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 ISO/IEC 27001:2013 certified to adopt MTCS SS, requirements listed in ISO/IEC 27001:2013 were mapped against equivalent requirements in MTCS SS. This followed a structured and systematic three (3) step approach:

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



7 Summary of Findings

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

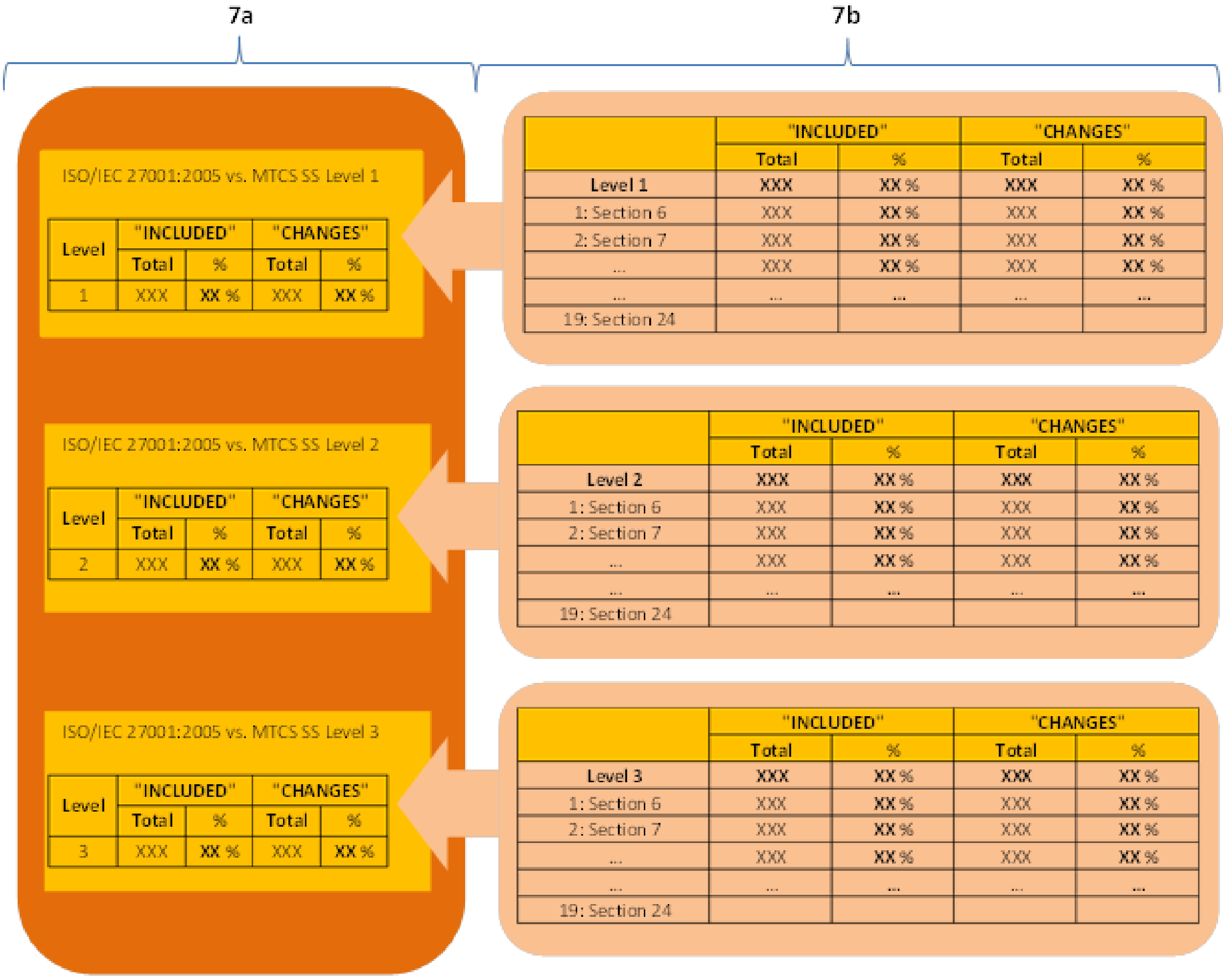
a. Summary by Levels in MTCS SS certification (Levels 1, 2 and 3)

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

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

Section 7.2 summarises the total gaps identified for ISO/IEC 27001:2013 as compared to each of the nineteen (19) areas for the three (3) levels in MTCS SS.

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



ISO/IEC 27001:2005 vs. MTCS SS Level 1

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

ISO/IEC 27001:2005 vs. MTCS SS Level 2

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

ISO/IEC 27001:2005 vs. MTCS SS Level 3

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

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

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

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

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

Column	Column description
Total Clauses*	Indicates the number of clauses that are currently listed in the MTCS SS. The Total is inclusive of the preceding Level's requirements, for example, Level 3 includes requirements in Levels 1 and 2.
INCLUDED	Indicates the number of clauses in the MTCS SS that are equally represented in ISO/IEC 27001:2013
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 MTCS SS that are stated with more details than the corresponding sections in clauses in ISO/IEC 27001:2013. In general, the requirements are classified as "INCREMENTAL" if the required enhancements on the existing ISO/IEC 27001:2013 characteristics are not costly or onerous in nature.
NEW	Indicates the number of clauses in the MTCS SS that are absent, or stated with significantly more details than the corresponding sections and clauses in ISO/IEC 27001:2013. In general, the requirements are classified as "NEW" if there may be material financial cost to meet relevant MTCS SS requirement, additional controls to be included in the audit checklist and / or the effort is relatively onerous.

*The word "Clause(s)" refer generally to both "Clause(s)" and "Sub-clause(s)" that specify control requirements.

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

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

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

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

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

Level	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 1	297	114	**38%**	183	**62%**	44	**15%**	139	**47%**

The table below provides a high level summary of the differences between MTCS SS Level 2 and ISO/IEC 27001:2013. Cloud Service Providers looking to be cross certified to MTCS SS Level 2 can refer to this table for total requirements applicable to this level. Note that the total clauses of 450 comprises of the 297 clauses in Level 1 and in addition, 153 unique Level 2 clauses.

Level	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 2	450	147	**33%**	303	**67%**	63	**14%**	240	**53%**

The table below provides a high level summary of the differences between MTCS SS Level 3 and ISO/IEC 27001:2013. Cloud Service Providers looking to be cross certified to MTCS SS Level 3 can refer to this table for total requirements applicable to this level. Note that the total clauses of 538 comprises of the 450 clauses in Level 2 and in addition, 88 unique Level 3 clauses.

Level	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 3	538	156	**29%**	382	**71%**	69	**13%**	313	**58%**

7.2 Summary by Control Areas

The purpose of this section is to provide an overview of the differences between the MTCS SS and ISO/IEC 27001:2013 Standard by Control Areas in MTCS SS Levels 1, 2 and 3. Cloud Service Providers that are ISO/IEC 27001:2013 certified and are interested in obtaining MTCS certification in Levels 1, 2 or 3 can view the key logical areas that require enhancements / upgrades in order to adopt MTCS SS.

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

Sections	Total Clauses	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	34	22	65%	12	35%	2	6%	10	29%
Section 7	10	8	80%	2	20%	0	0%	2	20%
Section 8	8	7	67%	1	13%	1	13%	0	0%
Section 9	7	5	71%	2	29%	1	14%	1	14%
Section 10	17	6	35%	11	65%	3	18%	8	47%
Section 11	17	0	0%	17	100%	7	41%	10	59%
Section 12	8	0	0%	8	100%	4	50%	4	50%
Section 13	13	1	8%	12	92%	4	31%	8	62%
Section 14	24	0	0%	24	100%	8	33%	16	67%
Section 15	6	1	17%	5	83%	1	17%	4	67%
Section 16	14	5	36%	9	64%	1	7%	8	57%
Section 17	14	0	0%	14	100%	1	7%	13	93%
Section 18	27	7	26%	20	74%	0	0%	20	74%
Section 19	3	1	33%	2	67%	0	0%	2	67%
Section 20	5	1	20%	4	80%	0	0%	4	80%
Section 21	11	1	9%	10	91%	0	0%	10	91%
Section 22	34	19	56%	15	44%	10	29%	5	15%
Section 23	23	16	70%	7	30%	1	4%	6	26%
Section 24	22	14	64%	8	36%	0	0%	8	36%
Level 1	**297**	**114**	**38%**	**183**	**62%**	**44**	**15%**	**139**	**47%**

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

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

The table below summarises the differences between MTCS SS Level 2 and ISO/IEC 27001:2013[1]. Additional control requirements for Level 2 are indicated in the parentheses:

Sections	Total Clauses	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	41	26(+4)	**64%**	15	**37%**	3(+1)	**7%**	12(+2)	**29%**
Section 7	20	13(+5)	**65%**	7	**35%**	0(0)	**0%**	7(+5)	**35%**
Section 8	16	13(+6)	**81%**	3	**19%**	3(+2)	**19%**	0(0)	**0%**
Section 9	10	7(+2)	**70%**	3	**30%**	1(0)	**10%**	2(+1)	**20%**
Section 10	21	9(+3)	**43%**	12	**57%**	3(0)	**14%**	9(+1)	**43%**
Section 11	24	0(0)	**0%**	24	**100%**	7(0)	**29%**	17(+7)	**71%**
Section 12	33	3(+3)	**9%**	30	**91%**	13(+9)	**39%**	17(+13)	**52%**
Section 13	22	1(0)	**5%**	21	**95%**	4(0)	**18%**	17(+9)	**77%**
Section 14	27	0(0)	**0%**	27	**100%**	8(0)	**30%**	19(+3)	**70%**
Section 15	8	1(0)	**12%**	7	**88%**	1(0)	**13%**	6(+2)	**75%**
Section 16	20	5(0)	**25%**	15	**75%**	1(0)	**5%**	14(+6)	**70%**
Section 17	22	0(0)	**0%**	22	**100%**	1(0)	**5%**	21(+8)	**95%**
Section 18	32	8(+1)	**25%**	24	**75%**	0(0)	**0%**	24(+4)	**75%**
Section 19	9	1(0)	**11%**	8	**89%**	0(0)	**0%**	8(+6)	**89%**
Section 20	12	1(0)	**8%**	11	**92%**	0(0)	**0%**	11(+7)	**92%**
Section 21	13	1(0)	**8%**	12	**92%**	0(0)	**0%**	12(+2)	**92%**
Section 22	50	21(+2)	**42%**	29	**58%**	12(+2)	**24%**	17(+12)	**34%**
Section 23	32	19(+3)	**59%**	13	**41%**	3(+2)	**9%**	10(+4)	**31%**
Section 24	38	18(+4)	**47%**	20	**53%**	3(+3)	**8%**	17(+9)	**45%**
Level 2	**450**	**147**	**33%**	**303**	**67%**	**63**	**14%**	**240**	**53%**

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

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

The table below summarises the differences between MTCS SS Level 3 and ISO/IEC 27001:2013[1]. Additional control requirements for Level 3 are indicated in the parentheses:

Sections	Total Clauses	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	43	28(+2)	**65%**	15	**35%**	3(0)	**7%**	12(0)	**28%**
Section 7	24	14(+1)	**58%**	10	**42%**	0(0)	**0%**	10(+3)	**42%**
Section 8	18	13(0)	**72%**	5	**28%**	3(0)	**17%**	2(+2)	**11%**
Section 9	17	9(+2)	**53%**	8	**47%**	2(+1)	**12%**	6(+4)	**35%**
Section 10	23	10(+1)	**43%**	13	**57%**	3(0)	**13%**	10(+1)	**43%**
Section 11	29	0(0)	**0%**	29	**100%**	7(0)	**24%**	22(+5)	**76%**
Section 12	38	3(0)	**8%**	35	**92%**	13(0)	**34%**	22(+5)	**58%**
Section 13	27	1(0)	**4%**	26	**96%**	4(0)	**15%**	22(+5)	**81%**
Section 14	32	0(0)	**0%**	32	**100%**	8(0)	**25%**	24(+5)	**75%**
Section 15	11	1(0)	**9%**	10	**91%**	1(0)	**9%**	9(+3)	**82%**
Section 16	22	5(0)	**23%**	17	**77%**	1(0)	**5%**	16(+2)	**73%**
Section 17	23	0(0)	**0%**	23	**100%**	1(0)	**4%**	22(+1)	**96%**
Section 18	32	8(0)	**25%**	24	**75%**	0(0)	**0%**	24(0)	**75%**
Section 19	26	1(0)	**4%**	25	**96%**	0(0)	**0%**	25(+17)	**96%**
Section 20	14	1(0)	**7%**	13	**93%**	0(0)	**0%**	13(+2)	**93%**
Section 21	20	1(0)	**5%**	19	**95%**	0(0)	**0%**	19(+7)	**95%**
Section 22	56	22(+1)	**39%**	34	**61%**	15(+3)	**27%**	19(+2)	**34%**
Section 23	34	20(+1)	**59%**	14	**41%**	4(+1)	**12%**	10(0)	**29%**
Section 24	49	19(+1)	**39%**	30	**61%**	4(+1)	**8%**	26(+9)	**53%**
Level 3	**538**	**156**	**29%**	**382**	**71%**	**69**	**13%**	**313**	**58%**

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

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

8 Tips on Using this Gap Analysis Report

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

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

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

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

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

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

Statements such as “No applicable Level 1 controls” and “No applicable Level 2 controls” denote that there are no applicable requirements or controls for that corresponding Level.

Statements such as “The requirement is the same as that in Level 1” and “The requirements are the same as that in Level 2” denote that there are no additional requirements specific to that level; on top of the requirements from the preceding level.

MTCS SS has several requirements where higher level supersedes those at lower level(s). Cloud Service Providers should note that they can only comply with requirements for the specific level in areas involving frequency of activities. For example, in MTCS SS Clause 15.1 ‘Vulnerability scanning’, Cloud Service Providers have to conduct vulnerability scanning more frequently if they are looking to be certified at the next level.

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

9 Gap Analysis

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

9.1 Information security management

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6 Information security management				
6.1 Information security management controls				
6.2 Information security management system (ISMS)				
6.2.1 General				
Control Objective	INCLUDED	4.4		
6.2.2 Level 1 requirements				
6.2.2(a)	INCLUDED		A.8.1 A.11.2	
6.2.2(b)	INCLUDED	6.1.1d 6.1.2 6.1.3		

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6.2.2(c)	INCLUDED	5.2		
6.2.2(d)	INCLUDED	5.3		
6.2.2(e)	INCLUDED		A.9.1 A.9.2 A.9.3	
6.2.2(f)	INCLUDED		A.9 A.12.4	
6.2.2(g)	INCLUDED		A.9.4	
6.2.2(h)	INCLUDED		A.14	
6.2.2(i)	NEW			
6.2.2(j)	NEW			
6.2.2(k)	INCLUDED		A.16.1.2 A.16.1.6	
6.2.3 Level 2 requirements				
6.2.3(a)	INCREMENTAL		A.12.3 A.12.4.2	
6.2.3(b)	INCLUDED	6.1.1e1 9.1	A.17.1.3	
6.2.4 Level 3 requirements				
6.2.4(a)	INCLUDED	4.4		

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6.2.4(b)	INCLUDED	4.3c 7.4		
6.3 Management of information security				
6.3.1 General				
Control Objective	INCLUDED	5 6.1.1	A.5	
6.3.2 Level 1 requirements				
6.3.2(a)	INCLUDED	5.3a	A.6.1.2	
6.3.2(b)	INCLUDED		A.6.1.1 A.6.1.5 A.7.2.1	
6.3.2(c)	INCLUDED		A.6.1.1 A.7.2.1	
6.3.2(d)	INCLUDED		A.15.1 A.15.2.1	
6.3.3 Level 2 requirements				
6.3.3(a)	INCLUDED	6.2h	A.6.1.1	
6.3.3(b)	INCLUDED	5.2e 7.5.1		
6.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.4 Management oversight of information security				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6.4.1 General				
Control Objective	NEW	5.1		ISO27001 requires this of the Organisation, not specifically Board of Directors
6.4.2 Level 1 requirements				
6.4.2(a)	NEW		A.5.1.1 A.6.1	ISO27001 requires this of the Organisation, not specifically Board of Directors
6.4.2(b)	NEW			ISO27001 requires this of the Organisation, not specifically Board of Directors
6.4.2(c)	NEW	6.1.3		ISO27001 requires this of the Organisation, not specifically Board of Directors
6.4.2(d)	NEW	9.3		ISO27001 requires this of the Organisation, not specifically Board of Directors
6.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
6.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.5 Information security policy				
6.5.1 General				
Control Objective	INCLUDED	5.2 5.2e		
6.5.2 Level 1 requirements				
6.5.2(a)	INCLUDED	5.2		
6.5.2(b)	NEW			Reference to “strategic plan”

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
6.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.6 Review of information security policy				
6.6.1 General				
Control Objective	INCLUDED	9.1 9.3		
6.6.2 Level 1 requirements				
6.6.2	INCREMENTAL			Requirement for Annual review
6.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
6.6.4 Level 3 requirements **The requirement is the same as that in Level 2.**				
6.7 Information security audits				
6.7.1 General				
Control Objective	NEW			Requirement of “auditable entities”
6.7.2 Level 1 requirements				
6.7.2(a)	NEW			Requirement for Audit Committee
6.7.2(b)	NEW			Requirement for Audit Committee
6.7.2(c)	NEW	9.2		Requirement for Annual
6.7.2(d)	INCREMENTAL	9.2d		

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6.7.2(e)	INCLUDED		A.8.2 A.9.1 A.9.2	
6.7.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
6.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.8 Information security liaisons (ISL)				
6.8.1 General				
Control Objective	INCLUDED		A.6.1.3	
6.8.2 Level 1 requirements				
6.8.2(a)	INCLUDED		A.6.1.3	
6.8.2(b)	INCLUDED		A.6.1.4	
6.8.2(c)	INCLUDED		A.6.1.4	
6.8.2(d)	INCLUDED	7.2c	A.7.2.2	
6.8.3 Level 2 requirements				
6.8.3	NEW			This implies the ISL is not a role
6.8.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.9 Acceptable Usage				
6.9.1 General				
Control Objective	INCLUDED		A.8.1.3	
6.9.2 Level 1 requirements				
6.9.2(a)	INCLUDED		A.14.1.1	
6.9.2(b)	INCLUDED		A.13.2.1d	

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
6.9.2(c)	INCLUDED	7.5		
6.9.3 Level 2 requirements				
6.9.3(a)	INCLUDED		A.8.2.1 A.8.2.2	
6.9.3(b)	NEW			
6.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.2 Human resources

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
7 Human resources				
7.1 Human resources security controls				
7.2 Background screening				
7.2.1 General				
Control Objective	INCLUDED		A.7.1.1	
7.2.2 Level 1 requirements				
7.2.2(a)	INCLUDED		A.7.1.1	
7.2.2(b)	INCLUDED		A.7.1.1	
7.2.3 Level 2 requirements				
7.2.3	INCLUDED		A.7.1.1	
7.2.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
7.2.4	INCLUDED		A.7.1.1	
7.3 Continuous personnel evaluation				
7.3.1 General				
Control Objective	NEW			Repeated background check is additional
7.3.2 Level 1 requirements **No applicable Level 1 controls.**				
7.3.3 Level 2 requirements				
7.3.3(a)	NEW			Repeated background check is additional
7.3.3(b)	NEW			Repeated background check is additional
7.3.4 Level 3 requirements				
7.3.4(a)	NEW			Repeated background check is additional
7.3.4(b)	NEW			Repeated background check is additional
7.4 Employment and contract terms and conditions				
7.4.1 General				
Control Objective	INCREMENTAL	7		MTCS requires additional controls
7.4.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
7.4.2(a)	INCLUDED	7.3c		
7.4.2(b)	INCLUDED	7.3c	A.7.1.2	
7.4.2(c)	INCLUDED		A.8.1.4 A.13.2.4 A.9.2.6	
7.4.2(d)	INCLUDED	7.3		
7.4.3 Level 2 requirements				
7.4.3(a)	NEW			Requirement for exit briefings
7.4.3(b)	NEW			Requirement for expedited timeframe
7.4.4 Level 3 requirements				
7.3.4	NEW			Annual re-acknowledgement
7.5 Disciplinary process				
7.5.1 General				
Control Objective	INCLUDED	7.3c	A.7.2.3	
7.5.2 Level 1 requirements				
7.5.2	INCLUDED	7.3c	A.7.2.3	
7.5.3 Level 2 requirements **The requirement is the same as that in Level 1.**				
7.5.4 Level 3 requirements **The requirement is the same as that in Level 2.**				
7.6 Asset returns				
7.6.1 General				
Control Objective	INCLUDED		A.8.1.4	
7.6.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
7.6.2	INCLUDED		A.8.1.4	
7.6.3 Level 2 requirements **The requirement is the same as that in Level 1.**				
7.6.4 Level 3 requirements **The requirement is the same as that in Level 2.**				
7.7 Information security training and awareness				
7.7.1 General				
Control Objective	INCLUDED	7.3	A.7.2.2	
7.7.2 Level 1 requirements				
7.7.2(a)	INCLUDED	7.3	A.7.2.2	
7.7.2(b)	INCLUDED	7.3	A.7.2.2 A.16.1.2 A.16.1.3	
7.7.3 Level 2 requirements				
7.7.3(a)	INCLUDED	7.3	A.7.2.2	
7.7.3(b)	INCLUDED	7.3	A.7.2.2	
7.7.3(c)	INCLUDED		A.7.1.2 A.15.1.2c	
7.7.3(d)	INCLUDED		A.18.1.4	
7.7.3(e)	NEW			Specific Normative Reference to Singapore Legislation

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
7.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.3 Risk management

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
8 Risk management				
8.1 Risk management controls				
8.2 Risk management program				
8.2.1 General				
Control Objective	INCLUDED	6.1 6.1.3		
8.2.2 Level 1 requirements				
8.2.2(a)	INCLUDED	6.1.3		
8.2.2(b)	INCLUDED	6.1.2c		
8.2.2(c)	INCLUDED	6.1.2d		
8.2.2(d)	INCLUDED	6.1.3		
8.2.2(e)	INCLUDED	6.1.3e 6.1.3f		
8.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
8.2.3	INCREMENTAL	6.1.3e 6.1.3f		Specific criteria requred
8.2.4 Level 3 requirements				
8.2.4	NEW	8.2		Quarterly review required
8.3 Risk assessment				
8.3.1 General				
Control Objective	NEW			Annual review required
8.3.2 Level 1 requirements				
8.3.2(a)	INCREMENTAL	6.1.2d	A.18.2.3	Threat and Impact Assessments
8.3.2(b)	INCLUDED	4.1 4.3		
8.3.2(c)	INCLUDED	6.1.2d		
8.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
8.3.3	INCLUDED		A.8.2.3 A.12.3 A18.1.3	
8.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
8.4 Risk management				
8.4.1 General				
Control Objective	INCLUDED	4.1 4.2 4.3 8.2 9.1		
8.4.2 Level 1 requirements **No applicable Level 1 controls.**				
8.4.3 Level 2 requirements				
8.4.3(a)	INCLUDED	8.2		
8.4.3(b)	INCLUDED	8.2		
8.4.3(c)	INCLUDED	8.3 9.1f 9.3e		
8.4.3(d)	INCLUDED	8.2		
8.4.3(e)	INCLUDED		A.16.1.6	
8.4.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
8.4.4	NEW			Specifies particular methodology
8.5 Risk register				
8.5.1 General				
Control Objective	INCLUDED	6.1.2		
8.5.2 Level 1 requirements **No applicable Level 1 controls.**				
8.5.3 Level 2 requirements				
8.5.3	INCREMENTAL	6.1.2 6.1.3		Specifies particular attributes of a Risk Register
8.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.4 Third party

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
9 Third-party				
9.1 Third-party security controls				
9.2 Third-party due diligence				
9.2.1 General				
Control Objective	INCLUDED	4.3c 5.2g 6.1.2c	A.13.1.2	
9.2.2 Level 1 requirements				
9.2.2(a)	INCLUDED		A.15.1	

9.2.2(b)	INCLUDED		A.15.1	
9.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
9.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
9.3 Identification of risks related to third parties				
9.3.1 General				
Control Objective	INCLUDED	4.3c 6.1.2c		
9.3.2 Level 1 requirements				
9.3.2	INCLUDED		A.15.2.1 A.15.2.2 A.18.1.1	
9.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
9.3.4 Level 3 requirements				
9.3.4(a)	NEW			TVRA on Third-Party
9.3.4(b)	NEW			Requirement of Third Party to have ISMS
9.4 Third-party agreement				
9.4.1 General				
Control Objective	INCREMENTAL		A.13.2.2 A.15	Inclusion of specific checklist
9.4.2 Level 1 requirements				
9.4.2	INCREMENTAL		A.13.2.2 A.15	Inclusion of specific checklist
9.4.3 Level 2 requirements				

9.4.3	NEW			Right to Audit Third Parties
9.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
9.5 Third-party delivery management				
9.5.1 General				
Control Objective	INCLUDED		A.15	
9.5.2 Level 1 requirements				
9.5.2(a)	INCLUDED		A.15.2.1	
9.5.2(b)	INCLUDED		A.15.2.2	
9.5.2(c)	NEW			This requires the entire upstream Supply Chain to be MTCS compliant.
9.5.3 Level 2 requirements				
9.5.3(a)	INCLUDED		A.15.1.3	
9.5.3(b)	INCLUDED		A.15.1.1	
9.5.4 Level 3 requirements				
9.5.4(a)	NEW		A.15.1.1	“High Standard” is new
9.5.4(b)	INCREMENTAL		A.15.2.1	Obtaining expert reports on suppliers’ compliance
9.5.4(c)	INCLUDED		A.15.2.1	

9.5.4(d)	NEW			Onsite visits to suppliers data centers
9.5.4(e)	INCLUDED		A.15.1.3	

9.5 Legal and compliance

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
10 Legal and compliance				
10.1 Legal and compliance controls				
10.2 Compliance with regulatory and contractual requirements				
10.2.1 General				
Control Objective	Included	A.18.1 Compliance with legal and contractual requirements		OK at high-level
10.2.2 Level 1 requirements				
10.2.2(a)	Included	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights		OK at high-level
10.2.2(b)	Included	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights		OK at high-level
10.2.2(c)	Included	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights		OK at high-level

10.2.3 Level 2 requirements				
10.2.3(a)	Included	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights A.18.1.4 Privacy and protection of personally identifiable information		OK at high-level
10.2.3(b)	Included	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights A.18.1.4 Privacy and protection of personally identifiable information		Ok at high-level
10.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
10.3 Compliance with policies and standards				
10.3.1 General				
Control Objective	Included	9.2 Internal Audit	A.18.2 Information security reviews	Ok at high-level
10.3.2 Level 1 requirements				

10.3.2	Included	9.2 Internal Audit	A.18.2 Information security reviews	Ok at high-level *(MTCS for this clause focuses on the need to have independent reviews and assessments to be performed for policies and standards.)* Note: If requirement is related to Internal Audit, refer to Clause 9.2 Internal Audit
10.3.3 Level 2 requirements				
10.3.3	Included	9.2 Internal Audit	A.18.2 Information security reviews	Ok at high-level *(MTCS for this clause focuses on the need to review the internal audit plans to ensure they reflect an examination of the compliance with the organisation's policies.)* Note: If requirement is related to Internal Audit, refer to Clause 9.2 Internal Audit
10.3.4 Level 3 requirements				

10.3.4	Included	9.2 Internal Audit	A.18.2 Information security reviews	Ok at high-level *(MTCS for this clause focuses on the need to perform 3rd party reviews and assessments on at least an annual basis.)* Note: If requirement is related to Internal Audit, refer to Clause 9.2 Internal Audit
10.4 Prevention of misuse of cloud facilities				
10.4.1 General				
Control Objective	New	NA		The CSP shall establish procedures, training or awareness and relevant policy enforcement actions to deter employees from unauthorised access and enforcement of commercial agreements with relevant 3rd parties and end uses.,
10.4.2 Level 1 requirements				
10.4.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to ensure employees and 3rd parties are aware of the precise scope of cloud environment; s permitted access and use.)*

10.4.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to ensure awareness of the monitoring in place.)*
10.4.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have Log-on warning message or reminder on access policies and.)*
10.4.2(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have monitoring to detect if the cloud infrastructure is being used a platform to attack others.)*
10.4.2(e)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to include access and monitoring policies / restrictions in contracts with 3rd parties.)*
10.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
10.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
10.5 Use of compliant cryptography controls				
10.5.1 General				

Control Objective	Incremental	A.10.1 Cryptographic		
10.5.2 Level 1 requirements				
10.5.2(a)	Incremental	A.10.1.1 Policy on the use of cryptographic controls		*In 27k, it only mentioned the need to establish policy on the cryptographic controls for protection of information Hence, it is non-prescriptive in implementation.* MTCS for this clause focuses on *framing & putting cryptographic controls* relevant agreements
10.5.2(b)	Incremental	A.10.1.1 Policy on the use of cryptographic controls		*In 27k, it only mentioned the need to establish policy on the cryptographic controls for protection of information Hence, it is non-prescriptive in implementation.* MTCS for this clause focuses on *knowledge and implementation of applicable laws and regulations* related to implementing cryptographic controls
10.5.2(c)	Incremental	A.10.1.1 Policy on the use of cryptographic controls		*In 27k, it only mentioned the need to establish policy on the cryptographic controls for protection of information Hence, it is non-prescriptive in implementation.* MTCS for this clause focuses on *knowledge and application of prevailing industry practices* related to implementing cryptographic controls

10.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
10.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
10.6 Third-party compliance				
10.6.1 General				
Control Objective	Incremental	A.15 Supplier service delivery management		Note: MTCS requires additional controls
10.6.2 Level 1 requirements				
10.6.2(a)	Included	A.15.1.1 Information security policy for supplier relationships		Ok at high-level Note: In 27k, they refer to third-party as supplier
10.6.2(b)	Included	A.15.1.2 Addressing security within supplier agreement A.15.1.3 Information and communication technology supply chain		Ok at high-level Note: In 27k, they refer to third-party as supplier
10.6.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have Data protection regulatory requirements specified in 3rd party contractual agreements.)*
10.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
10.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
10.7 Continuous compliance monitoring				
10.7.1 General				

Control Objective	New	NA		The CSP shall provide a mechanism for cloud users to perform continuous or real-time compliance monitoring
10.7.2 Level 1 requirements				
10.7.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have Data protection regulatory requirements specified in 3rd party contractual agreements.)*
10.7.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have event logs to be available for monitoring.)*
10.7.3 Level 2 requirements				
10.7.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have a mechanism to provide system access reports with an agreed upon timeframe to cloud users.)*
10.7.4 Level 3 requirements				

10.7.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to ensure CSC having real-time access to monitor security of the cloud environment specific to the type of cloud services provided.)*

9.6 Incident management

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11 Incident management				
11.1 Incident management controls				
11.2 Information security incident response plan and procedure				
11.2.1 General				
Control Objective	Incremental		A.16 Information security incident management	MTCS requires additional controls
11.2.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.2(a)	Incremental		A.16.1.1 Responsibilities and procedures	*In 27k, it only mentioned the need to establish management responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents.* MTCS for this clause focuses on the need to have the R&R of CSP and relevant parties supporting or providing cloud services *Note:* The standard is non-prescriptive in implementation.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.2(b)	Incremental		A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses A.16.1.5 Response to information security events	*In 27k, it only mentioned the need to report incident security event, information security weaknesses & information security incidents weaknesses. It is non-prescriptive in implementations.* MTCS for this clause focuses on *internal & external communication* and *contact procedures* in the event of a security breach
11.2.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have extent of cooperation defined in SLA and communicated to all relevant parties*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.2(d)	Incremental		A.16.1.4 Assessment of and decision on information security events	*In 27k, it only mentioned the need to assess information security events, evaluate it to determine if it is an information security incident. It is non-prescriptive in implementations.* MTCS for this clause focuses on the *relevant root cause analysis, impact analysis* and the corresponding *follow-up actions*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.2(e)	Incremental		A.16.1.2 Reporting information security events A.16.1.3 Reporting information security weaknesses A.16.1.5 Response to information security incidents	*In 27k, it only mentioned the need to assess information security events, evaluate it to determine if it is an information security incident. It is non-prescriptive in implementations.* MTCS for this clause focuses on the *definition* of information security incident response, escalation and recovery procedures together with resolution in time frames
11.2.2(f)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have mechanism to enable information security incidents ro be monitored & quantified in terms of types, volumes and costs.)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.2(g)	Incremental		A.16.1.4 Assessment of and decision on information security events	*In 27k, it only mentioned the need to assess information security events, evaluate it to determine if it is an information security incident. It is non-prescriptive in implementations.* MTCS for this clause focuses on the need to *classify incidents* by *potential severity* level and *prioritised* accordingly.
11.2.2(h)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to disclose any security breach to potentially affected customers.)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.2(i)	Incremental		A.16.1.7 Collection of evidence	*In 27k, it only mentioned the need to define & apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence* MTCS for this clause focuses on the capability of CSP to provide CSC with required digital forensic evidence
11.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have designated personnel to be available to respond to security alerts from intrusion detection, prevention & the file integrity monitoring system.)* Note: The closest clause could be linked to A.16.1.1. Responsibilities & procedures where designated personnel to handle security alerts may be defined here.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have follow applicable legal requirements for reporting security breaches)*
11.2.3(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have process to monitor and track all incidents to closure.)* Note: The closest clause could be linked to A.16.1.1. Responsibilities & procedures where processes are put in place to monitor and track all incidents to closure.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.3(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have process to escalate events, to contain and remediate the breach.)* Note: The closest clause could be linked to A.16.1.1. Responsibilities & procedures where processes are put in place for escalating events as required.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.3(e)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have process to identify customers and affected parties of incidents and the impact of incidents, including the planned course of action of remediation.)* Note: The closest clause could be linked to A.16.1.1. Responsibilities & procedures where processes are put in place to notify customers and affected parties of incidents and the impact of the incidents
11.2.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.4(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have formal overall strategy and safeguards in responding to botnet threats and DDOS)*
11.2.4(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have pre-determined action plan to address public relations issues)*
11.2.4(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to pre- report to affected customers on major incidents)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.2.4(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to follow proper forensic procedures in terms of collection, retention and presentation of evidence)*
11.3 Information security incident response plan testing and updates				
11.3.1 General				
Control Objective	New		A.16 Information security incident management	
11.3.2 Level 1 requirements				
11.3.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have Incident response test plan covering types of test, test scope and parties to be involved in the test execution and review)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.3.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have annual testing of Incident response test plan)*
11.3.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have appropriate training to peroneal assigned with information security incident responsibilities)*
11.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.3.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to identify any industry standard applicable for performing the incident response)* Note: The closest clause could be linked to A.16.1.1. Responsibilities & procedures where process could be put in place to maintain information security incident response plan up-to-date
11.3.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.3.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to have Incident drills with defined escalation response time and in-depth stakeholder's involvement and reporting shall be conducted at least twice a year)*
11.4 Information security incident reporting				
11.4.1 General				
Control Objective	Incremental		A.16 Information security incident management	
11.4.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.4.2(a)	Incremental		A.16.1.2 Reporting information security events	*In 27k, it only mentioned Information security events shall be reported through appropriate management channels as quickly as possible* MTCS for this clause focuses on the need to *notify appropriate management*, as soon as possible through predefined communication channels in a prompt and expedient manner
11.4.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to inform and provide support to the relevant cloud users and third parties affected by the security breach of information systems and services in a timely manner)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
11.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
11.5 Problem management				
11.5.1 General				
Control Objective	New	NA		The CSP shall establish clear processes and procedures to handle problems arising from incidents, including information security and mon-information security incidents
11.5.2 Level 1 requirements				
11.5.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to identify, classify, prioritise and address issues)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.5.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to establish clear roles & responsibilities for staff handling problem management)*
11.5.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to establish escalation process for problems with different severity levels)*
11.5.3 Level 2 requirements				
11.5.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to develop a quarterly trend analysis of past incidents to identify and rectify problems)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
11.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.7 Data governance

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12 Data governance				
12.1 Data governance control				
12.2 Data classification				
12.2.1 General				
Control Objective	Incremental	A.8.2 Information classification		Note: The CSP shall establish controls to secure data according to its classification and define relevant procedures
12.2.2 Level 1 requirements **No applicable Level 1 controls.**				
12.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.2.3(a)	Incremental		A.8.2.1 Classification of information	*In 27k, it only mentioned Information shall be classified in terms of legal requirements, value, criticality and sensitivity to authorised disclosure or modification* *(MTCS for this clause focuses on the implementation of controls in accordance to data classification, type of data, legal requirements, sensitivity and critically)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.2.3(b)	Incremental		A.8.2.1 Classification of information	*In 27k, it only mentioned Information shall be classified in terms of legal requirements, value, criticality and sensitivity to authorised disclosure or modification* *(MTCS for this clause focuses on the need to ensure media being classified according to the data type)*
12.2.3(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to ensure communication channels being classified)*
12.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.3 Data ownership				
12.3.1 General				
Control Objective	Incremental		A.8.1.2 Ownership of assets	

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.3.2 Level 1 requirements **No applicable Level 1 controls.**				
12.3.3 Level 2 requirements				
12.3.3	Incremental		A.8.1.2 Ownership of assets	*In 27k, it only mentioned the assets maintained in the inventory shall be owned* *(MTCS for this clause focuses on the need to ensure all data being designated with ownership (including responsibilities defined, assigned, documented and communicated))*
12.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.4 Data integrity				
12.4.1 General				
Control Objective	New			The CSP shall ensure data integrity on input/output, transmission or exchange of data in storage at all times.
12.4.2 Level 1 requirements **No applicable Level 1 controls.**				
12.4.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.4.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the implementation of validation checks on all input/output processes)*
12.4.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the embed controls to protect authenticity and message integrity)*
12.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.5 Data labeling / handling				
12.5.1 General				
Control Objective	Included		A.8.2.2 Labelling of information A.8.2.3 handling of assets	
12.5.2 Level 1 requirements **No applicable Level 1 controls.**				
12.5.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.5.3(a)	Included		A.8.2.2 Labelling of information A.8.2.3 Handling of assets	NA
12.5.3(b)	Included		A.8.1.1 Inventory of assets	
12.5.3(c)	Incremental		A.8.1.1 Inventory of assets	*In 27k, it only mentioned the need to identify and maintain inventory of assets* (MTCS for this clause focuses on the need *to determine how data is collected, processed, stored, transferred and deleted)*
12.5.3(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the need to specify clearly the location where data is stored)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.5.4 Level 3 requirements				
12.5.4(a)	New	NA		*There is no corresponding mapping for 27k (MTCS for this clause focuses on the maintaining of logs and inventories of physical location of CSC)*
12.5.4(b)	New	NA		*There is no corresponding mapping for 27k (MTCS for this clause focuses on documented procedure on how data is handled upon termination of service)*
12.6 Data protection				
12.6.1 General				
Control Objective	New			The CSP shall establish controls and procedures to protect data form loss and destruction by other tenants or by CSP authorised agents
12.6.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.6.2(a)	Incremental		A.8.3.1 Management of removable media	*In 27k, it only mentioned the need to implement procedure of removable media in accordance with the classification scheme* *(MTCS for this clause focuses on the detail of strict security controls over access to all media and virtualised images and snapshots)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.6.2(b)	New			*In 27k, it only mentioned the need to implement procedure of removable media in accordance with the classification scheme* *(MTCS for this clause focuses on the detail of Sufficient protection (e.g. inventory reflects current location, company providing transport is a recognised third party with associated controls, media is physically secured in tamper evident container, media has relevant encryption) Such controls shall be provisioned to physical media containing data, transported beyond the boundaries of the Cloud Service provider.)*
12.6.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.6.3(a)	Incremental		A.8.3.1 Management of removable media	*In 27k, it only mentioned the need to implement procedure of removable media in accordance with the classification scheme* *(MTCS for this clause focuses on security of the medial storage and the need to review at least annually)*
12.6.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on the implementation of security mechanisms to monitor sensitive data to prevent data leakage)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.6.3(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on to ensure end point devices handling customer data must be protected with strong encryption)*
12.6.3(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause focuses on:* *-detect & monitor any compromise of virtualised images & snapshots containing sensitive data* *-monitor the transmission of sensitive data from the virtualised images and snapshots to the internet)*
12.6.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.6.4	New	NA		*There is no corresponding mapping for 27k (MTCS for this clause focuses on the need to have data loss prevention strategy which address: Data at endpoint, Data in motion, Data at rest, Data leaving form the cloud network to the internet)*
12.7 Data retention				
12.7.1 General				
Control Objective	Incremental		A.12.3 Backup	
12.7.2 Level 1 requirements **No applicable Level 1 controls.**				
12.7.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.7.3(a)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated the backup need to *perform in accordance with legal, regulatory and business requirements*
12.7.3(b)	Included		A.12.3.1 Information backup	

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.7.3(c)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated the need *to perform secure data deletion or removal* when data is no longer needed

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.7.3(d)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated the need to have *periodic manual or automatic processes* to identify and delete all the data that exceeds defined retention requirements

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.7.3(e)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated the need to have provision of *sufficient retention period* of relevant logs that could potentially service as digital evidence as required by regulators
12.7.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.7.4(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to have mechanism for CSC to remove or destroy all data (including backups) in the event of contract termination either on expiry or prematurely)*
12.7.4(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to have provision of sufficient retention period of data as required by regulators)*
12.8 Data backups				
12.8.1 General				
Control Objective	Included		A.12.3.1 Information backup	

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.8.2 Level 1 requirements				
12.8.2(a)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated that *if back-ups are stored off-site, they will need to be protected before transpiration through encryption or other means*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.8.2(b)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated the need *to determine the frequency of testing required on the backups*
12.8.2(c)	Incremental		A.12.3.1 Information backup	*In 27k, it only mentioned the need to perform backup and testing copies of information, software and system images regularly in accordance with an agreed backup policy* MTCS for this clause has specifically indicated the need *to determine the access and storage locations of backup*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.8.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
12.8.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.9 Secure disposal and decommissioning of hardcopy, media and equipment				
12.9.1 General				
Control Objective	New	NA		The Cloud Service Provider shall establish and implement secure disposal and decommissioning procedures for the hardcopy, media and equipment. The procedures shall address, but not be limited to, the following requirements and audit procedures.
12.9.2 Level 1 requirements				
12.9.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure media is wiped or disposed* or securely *and safety when no longer required, using formal procedures)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.9.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to check that equipment and storage media containing any sensitive data and licensed software are securely overwritten and/or forensically erased prior disposal. Data shall not be retrievable using forensic mechanism*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.9.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to shred, incinerate or pulp hardcopy materials so that data cannot be reconstructed or obtain a "Certificate of Destruction" from a data disposal.*
12.9.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
12.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.10 Secure disposal verification of live instances and backups				
12.10.1 General				
Control Objective	New	NA		The CSP shall establish secure disposal verification procedures for live instance/snapshots, dormant VMs and backups
12.10.2 Level 1 requirements **No applicable Level 1 controls.**				
12.10.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.10.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to verify that data is removed from entire cloud environment including live instance/snapshots, dormant VMs and backups, when it is deleted)*
12.10.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.11 Tracking of data				
12.11.1 General				
Control Objective	New	NA		The Cloud Service Provider shall provide cloud service customers with a mechanism to track data.
12.11.2 Level 1 requirements **No applicable Level 1 controls.**				
12.11.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.11.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure locations of all data in production and backup environments are available)*
12.11.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.12 Production data				
12.12.1 General				
Control Objective	New	NA		CSP to put in controls to prevent migration of production data to systems that do not have the same or greater level controls
12.12.2 Level 1 requirements **No applicable Level 1 controls.**				
12.12.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.12.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure controls are in place to prohibit extracting or transferring production data to non-production media, systems, or environments that do not have the same controls as production)*
12.12.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to have internal approve process in place prior to duplication of production data)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
12.12.3(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to verify that the data sanitisation process is in place)*
12.12.3(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to verify that approvals have been obtained in such instances)*
12.12.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.8 Audit logging and monitoring

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13 Audit logging and monitoring				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.1 Audit logging and monitoring controls				
13.2 Logging and monitoring process				
13.2.1 General				
Control Objective	Incremental		A.12.4 Logging and monitoring	CSP needs to have process to track and monitor all access to network resources and system components
13.2.2 Level 1 requirements				
13.2.2(a)	Incremental		A.12.4.3 Administrator and operator logs	*In 27k, it only mentioned system administrator and system operator activities need to be logged and the logs to be protected and regularly reviewed* MTCS for this clause has specifically indicated the need to *enable audit trails of privileged administrators' access* on all system and network components

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.2(b)	Incremental		A.12.4.1 Event logging	*In 27k, it only mentioned that event logs recording user activities, exceptions, faults and information security events to be produced, kept and regularly reviewed* MTCS for this clause has specifically indicated the need to *enable fault logging*
13.2.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to enable logging on changes)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.2(d)	Incremental		A.12.4.1 Event logging	*In 27k, it only mentioned that event logs recording user activities, exceptions, faults and information security events to be produced, kept and regularly reviewed* MTCS for this clause has specifically indicated the need to *enable fault logging*
13.2.2(e)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to review audit trails regularly to detect any anomalies)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.2(f)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to review logging of identification and authentication mechanism usage, and initializing of audit trail files)*
13.2.2(g)	Included		A.12.4.4 Clock synchronisation	
13.2.2(h)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement procedures to monitor the use of information processing facilities and review the results regularly)*
13.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to enable audit trails of user's access on all system and network components in the cloud environment)*
13.2.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to review audit trails regularly to detect attempts of individual logical access)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.3(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to enable audit trails of creation and deletion of system-level objects)*
13.2.3(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement file integrity monitoring or change detection software on logs to generate alerts of changes are made to the audit trails)* *)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.3(e)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement real time network monitoring procedures using Intrusion Detection and Prevention Systems)*
13.2.4 Level 3 requirements				
13.2.4(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure real time monitoring on all critical infrastructures being implemented)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.4(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement real time network monitoring procedures using Intrusion Detection and Prevention Systems)*
13.2.4(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement real time network monitoring procedures using Intrusion Detection and Prevention Systems)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.2.4(d)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement real time network monitoring procedures using Intrusion Detection and Prevention Systems)*
13.3 Log review				
13.3.1 General				
Control Objective	Incremental		A.12.4.1 Event Logging	CSP shall have in place a process to review logs
13.3.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.3.2	Incremental		A.12.4.1 Event Logging	*In 27k, it only mentioned that event logs, recording user activities, exceptions, faults and information security events to be produced, kept and regularly reviewed* MTCS for this clause has specifically indicated the need to *perform log review for all system components periodically*
13.3.3 Level 2 requirements				
13.3.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to perform log review for all system components at least daily)*
13.3.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.3.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to implement an automation tool for real time/daily monitoring of logs)*
13.4 Audit trails				
13.4.1 General				
Control Objective	New	NA		The CSP shall ensure audit trails of all access to network resources and system components are captured and protected
13.4.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.4.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated that the audit trail to include the followings in the event: -User identification, Event type and origination, Date & time stamp, Attempt status-success or failure, Affected data, system component or resource identification)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.4.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to access to audit trail being restricted using physical and logical user access controls)*
12.4.3 Level 2 requirements				
12.4.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure audit trails being written to write-only media or a tamper resistant location that prevents modification)*
13.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
13.5 Backup and retention of audit trails				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.5.1 General				
Control Objective	New	NA		The CSP shall establish a log retention procedure.
13.5.2 Level 1 requirements				
13.5.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure audit trails recording privileged user access activities, authorised and unauthorised access attempts, system exceptions and information security being keep for an agreed period)*
13.5.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.5.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure audit trails being backed up regularly to a centralised log server or media accessible by authorised personnel only)*

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.5.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure logs for internet accessible systems being written onto a log server located on an internal network segment protected by firewall. The log server should not have remote access and require tightly controlled IDs)*
13.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
13.6 Usage logs				
13.6.1 General				
Control Objective	New	NA		The CSP shall ensure integrity and accuracy of the usage logs always
13.5.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
13.6.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to have CSP ensure the usage logs not modifiable with strict controls to files & directories permission.)*
13.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
13.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.9 Secure configuration

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
14 Secure configuration				
14.1 Secure configuration controls				
14.2 Server and network device configuration standards				
14.2.1 General				

Control Objective	New	NA		The Cloud Service Provider shall develop configuration standards for all system components and network devices (including virtualised images, snapshots and hypervisor). These standards shall be consistent with industry-accepted system hardening standards, and ensure secure configuration of devices.
14.2.2 Level 1 requirements				
14.2.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to:* *-Verifying that network device or server configuration files are secured and synchronised.* *-Change vendor-supplied defaults configuration settings before installing a system on the network* *-Ensure that the configurations of virtualised images, snapshots and hypervisor are hardened* *-Conduct periodic hypervisor log analysis, integrity checks, and self-integrity checks upon boot-up of hypervisors* *-Disable clipboard or file-sharing services* *)*
14.2.2(b)	New	NA		
14.2.2(c)	New	NA		
14.2.2(d)	New	NA		
14.2.2(e)	New	NA		
14.2.2(f)	**NEW**	N/A	N/A	MTCS control requirement is specific to secure lifecycle management of images/applications at edge nodes in CSP.
14.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				

14.2.4 Level 3 requirements				
14.2.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *-Only deploy systems and infrastructure that have been thoroughly tested & certified by an independent third party for security assurance (e.g. Common Criteria EAL4, ICSA Labs, ISO 15408 or ISO 11889).* *)*
14.3 Malicious code prevention				
14.3.1 General				
Control Objective	Incremental		A.12.2 Protection form malware	The Cloud Service Provider shall ensure implementation of the following requirements and audit procedures to prevent malicious code threats.
14.3.2 Level 1 requirements				
14.3.2(a)	Incremental		A.12.2.1 Control against malware	*In 27k, it only mentioned the need to implement detection, prevention and recovery controls to protect against malware* MTCS for this clause has specifically indicate the need to detect, prevent and recover *“malicious codes”* instead of “malware”
14.3.2(b)	Incremental		A.12.2.1 Control against malware	*In 27k, it only mentioned the need to implement detection, prevention and recovery controls to protect against malware* MTCS for this clause has specifically
14.3.2(c)	Incremental		A.12.2.1 Control against malware	
14.3.2(d)	Incremental		A.12.2.1 Control against malware	

14.3.2(e)	Incremental		A.12.2.1 Control against malware	indicate the need to ensure: -anti-malware solutions protect all systems (b) -all anti-malware solutions are capable of detecting, removing and protecting against common types of malicious software (c) -Implementing controls to ensure that all anti-malware solutions are current, actively running and generating audit trails. (d) -anti-malware solutions are updated at least on a daily basis or when the vendor releases a new update (e) -updates of anti-malware solutions, engines, or other related codes can be rolled-back or mitigated in the event that an anti-malware update causes system malfunctions (f) -Appropriate awareness procedures for administrators of cloud systems (g)
14.3.2(f)	Incremental		A.12.2.1 Control against malware	
14.3.2(g)	Incremental		A.12.2.1 Control against malware	
14.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.3.4 Level 3 requirements				
14.3.4(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *-Periodic testing of the prevention and detection capabilities and recovery procedures against malicious code.* *)*

14.3.4(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *-Any user provided code is sandboxed or isolated to ensure the underlying platform and other tenants are not affected by the same* *)*
14.4 Portable code				
14.4.1 General				
Control Objective	New	NA		The Cloud Service Provider shall ensure controls are in place to address the risks associated with portable code (code that is executed in a remote location).
14.4.2 Level 1 requirements				
14.4.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Configuration is implemented to ensure that authorised portable code operates in accordance with a documented and approved security policy, and unauthorised portable code is restricted.* *)*
14.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.5 Physical port protection				

14.5.1 General				
Control Objective	New	NA		The Cloud Service Provider shall ensure implementation of the following requirements and audit procedures for port protection.
14.5.2 Level 1 requirements				
14.5.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Physical access to diagnostic and configuration ports are controlled and restricted only to authorised personnel and applications.* *)*
14.5.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *All unused physical and / or logical ports shall be disabled.* *)*

14.5.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *The configuration of unused physical and / or logical ports to be removed and any configuration required for hardening will be applied.* *)*
14.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.6 Restrictions to system utilities				
14.6.1 General				
Control Objective	New	NA		The Cloud Service Provider shall restrict and tightly control the use of utility programs through the following requirements and audit procedures.
14.6.2 Level 1 requirements				
14.6.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Utility programs that might be capable of overriding system and application controls are restricted and tightly controlled.* *)*
14.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				

14.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.7 System and network session management				
14.7.1 General				
Control Objective	New	NA		The Cloud Service Provider shall ensure implementation of the following requirements and audit procedures to manage inactive sessions.
14.7.2 Level 1 requirements				
14.7.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Inactive sessions are shut down after a defined period of inactivity.* *)*
14.7.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.8 Unnecessary service and protocols				
14.8.1 General				
Control Objective	New	NA		The Cloud Service Provider shall configure system security parameters to prevent misuse of services and protocols.
14.8.2 Level 1 requirements				

14.8.2(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Enable only necessary and secure services, protocols, daemons, etc. as required for the functioning of the system.* *)*
14.8.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Disable services, protocols, daemons, etc. not required for the functioning of the system.* *)*
14.8.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Inactive sessions are shut down after a defined period of inactivity.* *)*
14.8.3 Level 2 requirements				

14.8.3	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Remove all unnecessary functionality, such as scripts, drivers, extra features, subsystems, file systems and unnecessary web servers.* *)*
14.8.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.9 Unauthorised software				
14.9.1 General				
Control Objective	Incremental		A.12.6.2 Restrictions on software installation	The Cloud Service Provider shall put in place controls to restrict use of unapproved or unauthorised software.
14.9.2 Level 1 requirements				
14.9.2	Incremental		A.12.6.2 Restrictions on software installation	*In 27k, it only mentioned the need to have the rules governing the installation of software by users being established and implemented* MTCS for this clause has specifically indicate the need to *"prevent unauthorised software installations on the systems"*
14.9.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.10 Enforcement checks				
14.10.1 General				

Control Objective	New	NA		The Cloud Service Provider shall perform compliance checks to ensure all security configurations are applied according to baseline standards
14.10.2 Level 1 requirements				
14.10.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Checks being performed regularly on security configurations.* *)*
14.10.3 Level 2 requirements				
14.10.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Checks being performed at least weekly on security configurations.* *)*
14.10.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Implement file integrity monitoring tools to compare and alert unauthorised modification of critical systems, configurations and content files.* *)*
14.10.4 Level 3 requirements				

14.10.4(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Checks being performed at least daily on security configurations.* *)*
14.10.4(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Implement file integrity monitoring tools to compare and alert immediately unauthorised modification of critical systems, configurations and content files.* *)*

9.10 Security testing and monitoring

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
15 Security testing and monitoring				
15.1 Security testing and monitoring controls				
15.2 Vulnerability scanning				
15.2.1 General				
Control Objective	New	NA		Conduct internal and external vulnerability scans when there are significant changes in the infrastructure or at regular intervals.
15.2.2 Level 1 requirements				

15.2.2(a)	Incremental		A.18.2.3 Technical compliance review	*In 27k, it only mentioned the need to ensure information systems being regularly reviewed for compliance with the organization's information security policies and standards* MTCS for this clause has specifically indicate the need to ensure: *"Vulnerability scanning being performed at least on a quarterly basis."*
15.2.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Vulnerabilities with a CVSS score of 7-10 are addressed within one week. This may include resolving vulnerabilities or putting in place compensating controls until such time as a fix can be implemented.* *)*
15.2.3 Level 2 requirements				
15.2.3(a)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Vulnerability scanning shall be performed at least on a quarterly basis and when significant changes occur to the environment.* *)*

15.2.3(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Vulnerabilities with a CVSS score of 4-6.9 are addressed within one month. This may include resolving vulnerabilities or putting in place compensating controls until such time as a fix can be implemented.* *)*
15.2.4 Level 3 requirements				
15.2.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Vulnerability scanning shall be performed at least on a monthly basis.* *)*
15.3 Penetration testing				
15.3.1 General				
Control Objective	New	NA		The Cloud Service Provider shall conduct network layer and application layer penetration testing from the Internet, Cloud Service Management Network, and Cloud Service Provider Internal Network when there are significant infrastructure changes or application upgrades or modifications or at regular intervals.
15.3.2 Level 1 requirements				

15.3.2	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Penetration testing is conducted at least on a yearly basis.* *)*
15.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
15.3.4 Level 3 requirements				
15.3.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Penetration testing is conducted at least twice annually, with at least one test executed by a qualified third party.* *)*
15.4 Security monitoring				
15.4.1 General				
Control Objective	New	NA		The Cloud Service Provider shall conduct network layer and application layer penetration testing from the Internet, Cloud Service Management Network, and Cloud Service Provider Internal Network when there are significant infrastructure changes or application upgrades or modifications or at regular intervals.
15.4.2 Level 1 requirements				

15.4.2(a)	Included		A.12.6.1 Management of technical vulnerabilities	
15.4.2(b)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Implement intrusion detection systems, and / or intrusion prevention systems to monitor traffic.* *)*
15.4.2(c)	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *Establish and maintain up-to-date policies on security principles for network intrusion, detection and prevention.* *)*
15.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
15.4.4 Level 3 requirements				

15.4.4	New	NA		*There is no corresponding mapping for 27k* *(MTCS for this clause has specifically indicated the need to ensure:* *The Cloud Service Provider to include the following in its security monitoring process:* *-Schedule and perform regular technical compliance reviews to ensure systems security is maintained per design;* *- Identify and establish technical depth and scope of the review, as well as the tools or methodologies to be followed;* *-Assess technical competencies of the personnel performing the reviews.* *)*

9.11 System acquisitions and development

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
16 System acquisitions and development				
16.1 System acquisitions and development controls				
16.2 Development, acquisition and release management				
16.2.1 General				
Control Objective	INCREMENTAL	A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities was not included in ISO27001 control.
16.2.2 Level 1 requirements				
16.2.2(a)	INCLUDED	A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	N/A
16.2.2(b)	NEW	N/A	N/A	N/A
16.2.2(c)	INCREMENTAL	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.	Removal of test accounts before production systems become active was not included.
16.2.2(d)	NEW	N/A	N/A	N/A
16.2.2(e)	INCLUDED	A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
16.2.2(f)	INCLUDED	A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	N/A
16.2.2(g)	INCLUDED	A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	N/A
16.2.2(h)	INCLUDED	A.14.1.1 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems	N/A
16.2.2(i)	NEW	N/A	N/A	N/A
16.2.2(j)	NEW	N/A	N/A	N/A
16.2.2(k)	NEW	N/A	N/A	N/A
16.2.3 Level 2 requirements				
16.2.3	NEW	N/A	N/A	N/A
16.2.4 Level 3 requirements				
16.2.4	NEW	N/A	N/A	N/A
16.3 Web application security				
16.3.1 General				
Control Objective	NEW	N/A	N/A	N/A
16.3.2 Level 1 requirements **No applicable Level 1 controls.**				
16.3.3 Level 2 requirements				
16.3.3(a)	NEW	N/A	N/A	N/A
16.3.3(b)	NEW	N/A	N/A	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
16.3.3(c)	NEW	N/A	N/A	N/A
16.3.4 Level 3 requirements				
16.3.4	NEW	N/A	N/A	N/A
16.4 System testing				
16.4.1 General				
Control Objective	NEW	N/A	N/A	N/A
16.4.2 Level 1 requirements				
16.4.2	NEW	N/A	N/A	N/A
16.4.3 Level 2 requirements				
16.4.3	NEW	N/A	N/A	N/A
16.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
16.5 Source code security				
16.5.1 General				
Control Objective	NEW	N/A	N/A	N/A
16.5.2 Level 1 requirements				
16.5.2	NEW	N/A	N/A	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
16.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
16.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
16.6 Outsourced software development				
16.6.1 General				
Control Objective	INCLUDED	A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	N/A
16.6.2 Level 1 requirements				
16.6.2	NEW	N/A	N/A	N/A
16.6.3 Level 2 requirements				
16.6.3	NEW	N/A	N/A	N/A
16.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.12 Encryption

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
17 Encryption				
17.1 Encryption and secure cryptographic key management				
17.2 Encryption policies and procedures				
17.2.1 General				
Control Objective	INCLUDED	A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	N/A
17.2.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
17.2.2(a)	INCREMENTAL	A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Requirements for key custodian; key rotation; key retirement and revocation; minimum encryption standards; acceptable usage of encryption were not included.
17.2.2(b)	NEW	N/A	N/A	N/A
17.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
17.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
17.3 Channel encryption				
17.3.1 General				
Control Objective	NEW	N/A	N/A	N/A
17.3.2 Level 1 requirements				
17.3.2(a)	NEW	N/A	N/A	N/A
17.3.2(b)	NEW	N/A	N/A	N/A
17.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
17.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
17.4 Key management				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
17.4.1 General				
Control Objective	NEW	N/A	N/A	N/A
17.4.2 Level 1 requirements				
17.4.2(a)	NEW	N/A	N/A	N/A
17.4.2(b)	NEW	N/A	N/A	N/A
17.4.2(c)	NEW	N/A	N/A	N/A
17.4.2(d)	NEW	N/A	N/A	N/A
17.4.3 Level 2 requirements				
17.4.3(a)	NEW	N/A	N/A	N/A
17.4.3(b)	NEW	N/A	N/A	
17.4.3(c)	NEW	N/A	N/A	
17.4.3(d)	NEW	N/A	N/A	
17.4.3(e)	NEW	N/A	N/A	
17.4.3(f)	NEW	N/A	N/A	
17.4.3(g)	NEW	N/A	N/A	
17.4.3(h)	NEW	N/A	N/A	
17.4.4 Level 3 requirements				
17.4.4	NEW	N/A	N/A	N/A
17.5 Electronic messaging security				
17.5.1 General				
Control Objective	INCLUDED	A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	N/A
17.5.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
17.5.2(a)	NEW	N/A	N/A	N/A
17.5.2(b)	NEW	N/A	N/A	N/A
17.5.2(c)	NEW	N/A	N/A	N/A
17.5.2(d)	NEW	N/A	N/A	N/A
17.5.2(e)	NEW	N/A	N/A	N/A
17.5.2(f)	NEW	N/A	N/A	N/A
17.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
17.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.13 Physical and environmental

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
18 Physical and environmental				
18.1 Physical and environmental security controls				
18.2 Asset management				
18.2.1 General				
Control Objective	NEW	N/A	N/A	N/A
18.2.2 Level 1 requirements				
18.2.2(a)	INCLUDED	1) A.8.1.1 Inventory of assets 2) A.8.1.2 Ownership of assets	1) Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. 2) Assets maintained in the inventory shall be owned.	N/A
18.2.2(b)	NEW	N/A	N/A	N/A
18.2.2(c)	NEW	N/A	N/A	N/A
18.2.2(d)	NEW	N/A	N/A	N/A
18.2.2(e)	INCLUDED	A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	N/A
18.2.2(f)	INCLUDED	A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	N/A
18.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
18.2.3(a)	NEW	N/A	N/A	N/A
18.2.3(b)	INCLUDED	A.11.2.7 Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	N/A
18.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.3 Off-site movement				
18.3.1 General				
Control Objective	NEW	N/A	N/A	N/A
18.3.2 Level 1 requirements				
18.3.2	INCLUDED	A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	N/A
18.3.3 Level 2 requirements				
18.3.3	NEW	N/A	N/A	N/A
18.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.4 Physical access				
18.4.1 General				
Control Objective	NEW	N/A	N/A	N/A
18.4.2 Level 1 requirements				
18.4.2(a)	NEW	N/A	N/A	N/A
18.4.2(b)	NEW	N/A	N/A	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
18.4.2(c)	INCLUDED	A.11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	N/A
18.4.2(d)	NEW	N/A	N/A	N/A
18.4.2(e)	INCLUDED	A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	N/A
18.4.3 Level 2 requirements				
18.4.3	NEW	N/A	N/A	N/A
18.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.5 Visitors				
18.5.1 General				
Control Objective	NEW	N/A	N/A	N/A
18.5.2 Level 1 requirements				
18.5.2(a)	NEW	N/A	N/A	N/A
18.5.2(b)	NEW	N/A	N/A	N/A
18.5.2(c)	NEW	N/A	N/A	N/A
18.5.2(d)	NEW	N/A	N/A	N/A
18.5.2(e)	NEW	N/A	N/A	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
18.5.3 Level 2 requirements				
18.5.3	NEW	N/A	N/A	N/A
18.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.6 Environmental threats and equipment power failures				
18.6.1 General				
Control Objective	NEW	N/A	N/A	N/A
18.6.2 Level 1 requirements				
18.6.2(a)	NEW	N/A	N/A	N/A
18.6.2(b)	NEW	N/A	N/A	N/A
18.6.2(c)	NEW	N/A	N/A	N/A
18.6.2(d)	NEW	N/A	N/A	N/A
18.6.2(e)	INCLUDED	A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	N/A
18.6.2(f)	NEW	N/A	N/A	N/A
18.6.2(g)	NEW	N/A	N/A	N/A
18.6.2(h)	NEW	N/A	N/A	N/A
18.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
18.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.7 Physical security review				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
18.7.1 General				
Control Objective	NEW	N/A	N/A	N/A
18.7.2 Level 1 requirements				
18.7.2(a)	NEW	N/A	N/A	N/A
18.7.2(b)	NEW	N/A	N/A	N/A
18.7.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
18.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.14 Operations

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
19 Operations				
19.1 Operations security controls				
19.2 Operations management policies and procedures				
19.2.1 General				
Control Objective	INCREMENTAL	A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Does not specify explicitly required for equipment maintenance and management of its cloud services' operations to ensure continuity and availability of its operations.
19.2.2 Level 1 requirements **No applicable Level 1 controls.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
19.2.3 Level 2 requirements				
19.2.3	NEW	N/A	N/A	N/A
19.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
19.3 Documentation of service operations and external dependencies				
19.3.1 General				
Control Objective	NEW	N/A	N/A	N/A
19.3.2 Level 1 requirements				
19.3.2	NEW	N/A	N/A	N/A
19.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
19.3.4 Level 3 requirements				
19.3.4	NEW	N/A	N/A	N/A
19.4 Capacity management				
19.4.1 General				
Control Objective	NEW	N/A	N/A	N/A
19.4.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
19.4.2(a)	NEW	N/A	N/A	N/A
19.4.2(b)	INCLUDED	A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	N/A
19.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
19.4.4 Level 3 requirements				
19.4.4	NEW	N/A	N/A	N/A
19.5 Service levels				
19.5.1 General				
Control Objective	NEW	N/A	N/A	N/A
19.5.2 Level 1 requirements **No applicable Level 1 controls.**				
19.5.3 Level 2 requirements				
19.5.3(a)	NEW	N/A	N/A	N/A
19.5.3(b)	NEW	N/A	N/A	N/A
19.5.3(c)	NEW	N/A	N/A	N/A
19.5.4 Level 3 requirements				
19.5.4(a)	NEW	N/A	N/A	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
19.5.4(b)	NEW	N/A	N/A	N/A
19.5.4(c)	NEW	N/A	N/A	N/A
19.5.4(d)	NEW	N/A	N/A	N/A
19.5.4(e)	NEW	N/A	N/A	N/A
19.5.4(f)	NEW	N/A	N/A	N/A
19.6 Reliability and resiliency				
19.6.1 General				
Control Objective	NEW	N/A	N/A	N/A
19.6.2 Level 1 requirements **No applicable Level 1 controls.**				
19.6.3 Level 2 requirements **No applicable Level 2 controls.**				
19.6.4 Level 3 requirements				
19.6.4(a)	NEW	N/A	N/A	N/A
19.6.4(b)	NEW	N/A	N/A	N/A
19.6.4(c)	NEW	N/A	N/A	N/A
19.6.4(d)	NEW	N/A	N/A	N/A
19.6.4(e)	NEW	N/A	N/A	N/A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
19.6.4(f)	NEW	N/A	N/A	N/A
19.6.4(g)	NEW	N/A	N/A	N/A
19.6.4(h)	NEW	N/A	N/A	N/A
19.6.4(i)	**NEW**	N/A	N/A	N.A.
19.7 Recoverability				
19.7.1 General				
Control Objective	NEW	N/A	N/A	N/A
19.7.2 Level 1 requirements **No applicable Level 1 controls.**				
19.7.3 Level 2 requirements				
19.7.3(a)	NEW	N/A	N/A	N/A
19.7.3(b)	NEW	N/A	N/A	N/A
19.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.15 Change management

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
20 Change management				
20.1 Change management controls				
20.2 Change management process				
20.2.1 General				

Control Objective	INCREMENTAL	A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Does not specify explicitly on examples of changes include: a) System and security configuration changes; b) Hardware devices and security patches; c) Software updates; d) Creation, storage and use of virtualised images and snapshots.
20.2.2 Level 1 requirements				
20.2.2	NEW	N/A	N/A	N/A
20.2.3 Level 2 requirements				
20.2.3(a)	NEW	N/A	N/A	N/A
20.2.3(b)	NEW	N/A	N/A	N/A
20.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
20.3 Backup procedures				
20.3.1 General				
Control Objective	NEW	N/A	N/A	N/A
20.3.2 Level 1 requirements				

20.3.2	NEW	N/A	N/A	N/A
20.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
20.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
20.4 Back-out or rollback procedures				
20.4.1 General				
Control Objective	NEW	N/A	N/A	N/A
20.4.2 Level 1 requirements **No applicable Level 1 controls.**				
20.4.3 Level 2 requirements				
20.4.3	NEW	N/A	N/A	N/A
20.4.4 Level 3 requirements				
20.4.4	NEW	N/A	N/A	N/A
20.5 Separation of environment				
20.5.1 General				
Control Objective	INCLUDED	A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	N/A
20.5.2 Level 1 requirements				
20.5.2	INCLUDED	A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	N/A
20.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				

20.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
20.6 Patch management procedures				
20.6.1 General				
Control Objective	NEW	N/A	N/A	N/A
20.6.2 Level 1 requirements				
20.6.2(a)	NEW	N/A	N/A	N/A
20.6.2(b)	NEW	N/A	N/A	N/A
20.6.3 Level 2 requirements				
20.6.3(a)	NEW	N/A	N/A	N/A
20.6.3(b)	NEW	N/A	N/A	N/A
20.6.3(c)	NEW	N/A	N/A	N/A
20.6.3(d)	NEW	N/A	N/A	N/A
20.6.4 Level 3 requirements				
20.6.4	NEW	N/A	N/A	N/A

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

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
21 Business continuity planning (BCP) and disaster recovery (DR)				
21.1 BCP and DR controls				
21.2 BCP framework				
21.2.1 General				
Control Objective	NEW	N/A	N/A	N/A
21.2.2 Level 1 requirements				
21.2.2(a)	NEW	N/A	N/A	N/A
21.2.2(b)	NEW	N/A	N/A	N/A
21.2.2(c)	NEW	N/A	N/A	N/A
21.2.2(d)	NEW	N/A	N/A	N/A
21.2.2(e)	NEW	N/A	N/A	N/A
21.2.2(f)	NEW	N/A	N/A	N/A
21.2.3 Level 2 requirements				
21.2.3(a)	NEW	N/A	N/A	N/A
21.2.3(b)	NEW	N/A	N/A	N/A
21.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
21.3 BCP and DR plans				
21.3.1 General				
Control Objective	INCREMENTAL	A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Does not specify explicitly the requirements and audit procedures listed in 21.2.2.

21.3.2 Level 1 requirements				
21.3.2(a)	NEW	N/A	N/A	N/A
21.3.2(b)	NEW	N/A	N/A	N/A
21.3.2(c)	NEW	N/A	N/A	N/A
21.3.2(d)	NEW	N/A	N/A	N/A
21.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
21.3.4 Level 3 requirements				
21.3.4(a)	NEW	N/A	N/A	N/A
21.3.4(b)	NEW	N/A	N/A	N/A
21.3.4(c)	NEW	N/A	N/A	N/A
21.3.4(d)	NEW	N/A	N/A	N/A
21.4 BCP and DR testing				
21.4.1 General				
Control Objective	INCLUDED	A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	N/A
21.4.2 Level 1 requirements				

21.4.2	INCLUDED	A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	N/A
21.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
21.4.4 Level 3 requirements				
21.4.4(a)	NEW	N/A	N/A	N/A
21.4.4(b)	NEW	N/A	N/A	N/A
21.4.4(c)	NEW	N/A	N/A	N/A

9.17 Cloud services administration

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
22 Cloud services administration				
22.1 Cloud services administration controls				
22.2 Privilege account creation				
22.2.1 General				
Control Objective	**INCLUDED**	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	NA
22.2.2 Level 1 requirements				
22.2.2(a)	**INCLUDED**	A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights	NA
22.2.2(b)	**INCLUDED**	A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights	NA
22.2.2(c)	**INCLUDED**	A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	NA
22.2.2(d)	**INCLUDED**	9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	NA

22.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
22.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.3 Generation of administrator passwords				
22.3.1 General				
Control Objective	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	Note: Password management in general, rather than specific to administrator passwords
22.3.2 Level 1 requirements				
22.3.2(a)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
22.3.2(b)	INCLUDED	A.9.3.1 Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	NA
22.3.2(c)	INCLUDED	A.9.3.1 Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	NA
22.3.3 Level 2 requirements				
22.3.3(a)	NEW	N/A	N/A	MTCS strictly defines the password parameters.
22.3.3(b)	NEW	N/A	N/A	MTCS is specific on administrator accounts having Two-Factor Authentication (2FA) solution.
22.3.3(c)	NEW	N/A	N/A	MTCS is specific on administrators' 2FA solution being implemented based on the recommended practices.
22.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.4 Administrator access review and revocation				
22.4.1 General				
Control Objective	INCLUDED	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	NA
22.4.2 Level 1 requirements				

22.4.2(a)	INLCUDED	A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	NA
22.4.2(b)	INCLUDED	A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.	NA
22.4.2(c)	INCREMENTAL	A.9.2.5 Review of user access rights	Asset owners should review users' access rights at regular intervals.	MTCS requires the removal or disabling of inactive accounts at least every 90 days and notify relevant parties.
22.4.2(d)	INCLUDED	A.9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	NA
22.4.3 Level 2 requirements				
22.4.3	**INCLUDED**	A.7.2.1 Management responsibilities A.16.1.2 Reporting information security events A.16.1.5 Response to information security incidents	-Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. -Information security events should be reported through appropriate management channels as quickly as possible. -Information security incidents should be responded to in accordance with the documented procedures.	NA
22.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.5 Account lockout				
22.5.1 General				

Control Objective	INCREMENTAL	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	A.9.4.2 e) protect against brute force log-on attempts; f) log unsuccessful and successful attempts; g) raise a security event if a potential attempted or successful breach of log-on controls is detected; See details below for the other clauses
22.5.2 Level 1 requirements				
22.5.2(a)	INCREMENTAL	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS recommends account lockout after 6 unsuccessful attempts
22.5.2(b)	NEW	N/A	N/A	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS specifies user ID lockout duration to be a minimum of 30 minutes.
22.5.3 Level 2 requirements				
22.5.3	NEW	N/A	N/A	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS specifies that account shall be locked out until unlocked with commensurate controls.
22.5.3 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.6 Password change				
22.6.1 General				
Control Objective	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
22.6.2 Level 1 requirements				
22.6.2(a)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA

22.6.2(b)	INCREMENTAL	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	ISO 27k does not defined that password should be different from the three previous passwords, but it specifies to prevent password re-use. Refer A.9.4.3, f.
22.6.3 Level 2 requirements				
22.6.3	NEW	N/A	N/A	MTCS defines use of 2FA or token changes, which is not defined in ISO 27k
22.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.7 Password reset and first logon				
22.7.1 General				
Control Objective	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
22.7.2 Level 1 requirements				
22.7.2(a)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
22.7.2(b)	NEW	N/A	N/A	Note: ISO 27K, does not mentioned to verify first the identity prior to changing password
22.7.2(c)	NEW	N/A	N/A	Note: ISO 27K, did not mentioned policy on password reset
22.7.2(d)	NEW	N/A	N/A	Note: ISO 27k, did not specify implementation of secon factor authentication
22.7.3 Level 2 requirements				
22.7.3	NEW	N/A	N/A	MTCS specify new password should be split controlled and via out-of-band mechanism
22.7.4 Level 3 requirements				
22.7.4	NEW	N/A	N/A	MTCS specify new password should be split controlled and via out-of-band mechanism
22.8 Administrator access security				
22.8.1 General				

Control Objective	NEW	N/A	N/A	ISO 27K did not specify the administration of cloud infrastructure from unauthorised changes.
22.8.2 Level 1 requirements				
22.8.2(a)	NEW	N/A	N/A	MTCS specified that Cloud Service Provider shall only access Internal network to the cloud service management from specific IP Addresses.
22.8.2(b)	INCREMENTAL	A.6.2.1 Mobile device policy	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	ISO27k mentioned the registration of mobile devices.
22.8.2(c)	INCLUDED	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	NA
22.8.2(d)	INCLUDED	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	NA
22.8.2(e)	INCLUDED	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	NA
22.8.3 Level 2 requirements				
22.8.3	NEW	N/A	N/A	MTCS specified that access from Cloud Service Provide is only permitted via bastion host.
22.8.4 Level 3 requirements				
22.8.4	INCLUDED	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	NA
22.9 Administrator access logs				
22.9.1 General				
Control Objective	INCREMENTAL	A.12.4.3 Administrator and operator logs	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	Note: on a high-level ISO 27K states need to review system and activity logs regularly
22.9.2 Level 1 requirements				
22.9.2	INCREMENTAL	A.12.4.3 Administrator and operator logs	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	Note: on a high-level ISO 27K states need to review system and activity logs regularly
22.9.3 Level 2 requirements				

22.9.3	INCREMENTAL	A.12.4.2 Protection of log information A.12.4.1 Event logging	-Logging facilities and log information should be protected against tampering and unauthorized access. -Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Note: ISO 27K specifies logging facilities should be protected against tampering and unauthorized access.
22.9.4 Level 3 requirements				
22.9.4	INCREMENTAL	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Note: on a high level ISO 27K states need to event logs such as system activities, use of privileges should be recorded
22.10 Session management				
22.10.1 General				
Control Objective	INCREMENTAL	A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	See clauses below
22.10.2 Level 1 requirements				
22.10.2(a)	INCLUDED	A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	Note: On a high level ISO 27K clause A.9.4.2 that session will be deactivate if activity is idle for a period of time
22.10.2(b)	NEW	N/A	N/A	ISO 27K did not specify that password should be re-entered to reactivate terminal session
22.10.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
22.10.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.11 Segregation of duties				
22.11.1 General				
Control Objective	INCLUDED	A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	NA
22.11.2 Level 1 requirements				
22.11.2(a)	INCREMENTAL	A.9.1.1 Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	Note: ISO 27K did not mention the frequency of the segregation of duties risk review

22.11.2(b)	INCLUDED	A.12.1.4 Separation of development, testing and operational environments	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	NA
22.11.2(c)	INCREMENTAL	A.9.4.1 Information access restriction A.14.2.6 Secure development environment	-Access to information and application system functions should be restricted in accordance with the access control policy. -Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Note: ISO 27K, did not directly states the restriction of access to backup and production system, but might be in-scope with clause A.9.4.1 and A.14.2.6
22.11.3 Level 2 requirements				
22.11.3	INCREMENTAL	A.9.1.1 Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	Note: ISO 27K did not mention the frequency of the segration of duties risk review
22.11.4 Level 3 requirements				
22.11.4	INCREMENTAL	A.9.1.1 Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	Note: ISO 27K did not mention the frequency of the segration of duties risk review
22.12 Secure transmission of access credentials				
22.12.1 General				
Control Objective	INCLUDED	A.9.2.4 Management of secret authentication information of users	The allocation of secret authentication information should be controlled through a formal management process.	NA
22.12.2 Level 1 requirements				
22.12.2	INCLUDED	A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	NA
22.12.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
22.12.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.13 Third party administrative access				
22.13.1 General				

Control Objective	INCREMENTAL	A.9.2.3 Management of privileged access rights A.15.1.1 Information security policy for supplier relationships	The allocation and use of privileged access rights should be restricted and controlled. Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.	See clauses below
22.13.2 Level 1 requirements				
22.13.2(a)	INCREMENTAL	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	ISO 27K does not specifically mentioned privilege access restriction to vendors.
22.13.2(b)	INCLUDED	A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.	NA
22.13.3 Level 2 requirements				
22.13.3	NEW	N/A	N/A	MTCS specify to monitor and terminate activation of remote access services to third parties
22.13.4 Level 3 requirements				
22.13.4	NEW	N/A	N/A	MTCS is specific to only allow third party access to the environment under the direct supervision of the Cloud Service Provider
22.14 Service and application accounts				
22.14.1 General				
Control Objective	INCREMENTAL	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	See clauses below
22.14.2 Level 1 requirements				

22.14.2	INCREMENTAL	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	MTCS specifies that all service and application accounts created: Shall not be hardcoded, or stored as plain text within scripts, batch files, configurations, etc.; Shall not have the ability to log in interactively.
22.14.3 Level 2 requirements				
22.14.3(a)	NEW	N/A	N/A	MTCS is specific to implement one of the following controls to create service accounts: Dual password control (controlled by at least two administrators); One-use or time-limited administrator passwords.
22.14.3(b)	NEW	N/A	N/A	MTCS is specific to No caching or storing of sensitive session parameters, cookies or similar on local machines.
22.14.3(c)	NEW	N/A	N/A	MTCS is specific to restrict simultaneous logins.
22.14.3(d)	NEW	N/A	N/A	MTCS is specific to restrict console login access.
22.14.3(e)	NEW	N/A	N/A	MTCS says that Applications shall be developed by taking into consideration the cloud authentication model(i.e. native support of cloud authentication protocols or mechanisms).
22.14.4 Level 3 requirements				
22.14.4	INCREMENTAL	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	MTCS specified to change service account passwords at least twice annually.

9.18 Cloud user access

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23 Cloud user access				
23.1 Cloud user access controls				
23.2 User access registration				
23.2.1 General				
Control Objective	INCLUDED	A. 9.1.1 Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	NA
23.2.2 Level 1 requirements				
23.2.2(a)	INCLUDED	A.9.2.1 User registration and de-registration	A formal user registration and de-registration process should be implemented to enable assignment of access rights.	NA
23.2.2(b)	INCLUDED	A. 9.2.2 User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	NA
23.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
23.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.3 User access security				
23.3.1 General				
Control Objective	INCREMENTAL	A.9.2.2 User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	See clauses below
23.3.2 Level 1 requirements				
23.3.2(a)	INCLUDED	A.9.2.2 User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	NA

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.3.2(b)	INCLUDED	A. 12.4.2 Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	NA
23.3.2(c)	NEW	N/A	N/A	MTCS is specific to enforcing a default "deny-all" setting.
23.3.2(d)	INCLUDED	A. 14.1.2 Securing application services on public networks	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	NA
23.3.2(e)	NEW	N/A	N/A	MTCS is specific to anti-bot controls to foil automated brute force attacks. ISO27k only mentions a good log-on procedure should protect against brute force log-on attempts.
23.3.3 Level 2 requirements				
23.3.3	NEW	N/A	N/A	MTCS is specific on users having Two-Factor Authentication (2FA) solution.
23.3.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.3.4	INCREMENTAL	N/A	N/A	ISO 27K mentioned in 9.2.1 that the process for managing user IDs should include:: c) periodically identifying and removing or disabling redundant user IDs; d) ensuring that redundant user IDs are not issued to other users. MTCS is specific to federated identity management
23.4 User access password				
23.4.1 General				
Control Objective	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
23.4.2 Level 1 requirements				
23.4.2(a)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
23.4.2(b)	INCLUDED	A.9.3.1 Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	NA
23.4.2(c)	INCLUDED	A.9.3.1 Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	NA
23.4.3 Level 2 requirements				
23.4.3	NEW	N/A	N/A	MTCS strictly defines the password parameters.
23.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.5 User account lockout				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.5.1 General				
Control Objective	INCREMENTAL	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	NA
23.5.2 Level 1 requirements				
23.5.2(a)	INCREMENTAL	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS recommends account lockout after 6 unsuccessful attempts
23.5.2(b)	NEW	N/A	N/A	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS specifies user ID lockout duration to be a minimum of 30 minutes.
23.5.3 Level 2 requirements				
23.5.3(a)	INCREMENTAL	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS recommends account lockout after 6 unsuccessful attempts

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.5.3(b)	NEW	N/A	N/A	ISO 27K mentioned that a good log-on procedure should protect against brute force log-on attempts. MTCS specifies user ID lockout duration to be a minimum of 30 minutes.
23.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.6 User password reset and 1st logon change				
23.6.1 General				
Control Objective	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
23.6.2 Level 1 requirements				
23.6.2(a)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
23.6.2(b)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
23.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
23.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.7 Password protection				
23.7.1 General				
Control Objective	INCLUDED	A. 9.4.2 Secure log-on procedures A. 9.4.3 Password management system	A.9.4.2 Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure. A.9.4.3 Password management systems should be interactive and should ensure quality passwords.	INCLUDED
23.7.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.7.2(a)	INCLUDED	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	INCLUDED
23.7.2(b)	INCLUDED	A. 9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	INCLUDED
23.7.2(c)	INCLUDED	A. 9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	INCLUDED
23.7.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
23.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.8 User session management				
23.8.1 General				
Control Objective	INCREMENTAL	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	See clauses below
23.8.2 Level 1 requirements				
23.8.2(a)	INCLUDED	A. 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	NA
23.8.2(b)	NEW	N/A	N/A	MTCS is specific to re-entering password to reactivate terminal after session idle time for more than 15 minutes.
23.8.2(c)	NEW	N/A	N/A	MTCS is specific to implementing cryptographically strong session identifiers.
23.8.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.8.3	INCLUDED	A. 15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.	NA
23.8.4 Level 3 requirements				
23.8.4	INCLUDED	A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	NA
23.9 Change of cloud user's administrator details notification				
23.9.1 General				
Control Objective	NEW	N/A	N/A	See details below
23.9.2 Level 1 requirements **No applicable Level 1 controls**				
23.9.3 Level 2 requirements				
23.9.3(a)	NEW	N/A	N/A	MTCS specifies that cloud user's administrator details shall trigger an alert to the Cloud Service Provider's administrator.
23.9.3(b)	INCLUDED	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	NA
23.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.10 Self-service portal creation and management of user accounts				
23.10.1 General				
Control Objective	INCLUDED	A.9.2.2 User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	NA
23.10.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.10.2(a)	INCLUDED	A.9.4.3 Password management system	Password management systems should be interactive and should ensure quality passwords.	NA
23.10.2(b)	INCLUDED	A.9.2.2 User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	NA
23.10.3 Level 2 requirements				
23.10.3	INCLUDED	A.9.2.2 User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	NA
23.10.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.11 Communication with cloud users				
23.11.1 General				
Control Objective	INCREMENTAL	A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	See details below
23.11.2 Level 1 requirements				
23.11.2	NEW	N/A	N/A	ISO27K does not mention method for securely distributing official notifications
23.11.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
23.11.3	INCREMENTAL	A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	ISO27K does not mention awareness/education to customers
23.11.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.19 Tenancy and customer isolation

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2013 clauses	Reference to matching ISO/IEC 27001:2013 annex A reference control objectives and controls	Remarks on identified gaps
24 Tenancy and customer isolation				
24.1 Tenancy and customer isolation controls				
24.2 Multi tenancy				
24.2.1 General				
Control Objective	INCREMENTAL	A.13.1.3 Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	See details below
24.2.2 Level 1 requirements				
24.2.2(a)	INCLUDED	A.13.1.3 Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	NA
24.2.2(b)	INCLUDED	9.1.1 Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	9.1.1, e) management of access rights in a distributed and networked environment which recognizes all types of connections available;

24.2.2(c)	**NEW**	N/A	N/A	MTCS is specific to enforcing segregation between virtual machines belonging to different cloud service customers to prevent contagion effect of changes applied to a specific cloud service customer's virtual machine from spreading to other cloud service customers' virtual machines.
24.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
24.2.4 Level 3 requirements				
24.2.4(a)	**NEW**	N/A	N/A	MTCS is specific on implementing monitoring mechanisms to detect if one virtual host attempts to access another virtual host.
24.2.4(b)	**NEW**	N/A	N/A	MTCS is specific on ensuring virtual hosts with different security profiles are not hosted on the same system.
24.2.4(c)	**NEW**	N/A	N/A	MTCS is specific on ensuring communication between virtual hosts that is going outside of each cloud service customer shall pass through a firewall (or equivalent) configured to only allow the minimum traffic required.
24.3 Supporting infrastructure segmentation				
24.3.1 General				
Control Objective	**NEW**	N/A	N/A	ISO27k mentioned that on a highlevel, groups of information services, users and information systems should be segregated on networks.
24.3.2 Level 1 requirements **No applicable Level 1 controls**				
24.3.3 Level 2 requirements				

24.3.3(a)	NEW	N/A	N/A	MTCS is specific on authentication sources for Cloud Service Delivery Networks and the Cloud Service Provider Internal Networks being separated.
24.3.3(b)	INCREMENTAL	A.13.1.3 Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	ISO27k mentioned that on a high level, groups of information services, users and information systems should be segregated on networks.
24.3.3(c)	NEW	N/A	N/A	MTCS is specific on cloud Management Networks and Cloud Service Provider Internal Networks being segmented and no direct access is permitted, except via controlled access point with 2-factor authentication.
24.3.4 Level 3 requirements				
24.3.4	INCREMENTAL	A.13.1.3 Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	ISO27k mentioned that on a high level, groups of information services, users and information systems should be segregated on networks.
24.4 Network protection				
24.4.1 General				
Control Objective	INCLUDED	A.13.1 Network security management	To ensure the protection of information in networks and its supporting information pro-cessing facilities.	NA
24.4.2 Level 1 requirements				
24.4.2(a)	NEW	N/A	N/A	NA
24.4.2(b)	INCLUDED	A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	NA

24.4.2(c)	INCLUDED	A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	NA
24.4.2(d)	INCLUDED	A.14.2.5 Secure system engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.	NA
24.4.2(e)	INCLUDED	A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	NA
24.4.2(f)	NEW	N/A	N/A	MTCS is specific to high risk environments and data flow network diagrams.
24.4.2(g)	INCLUDED	A.9.1.2 Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	NA
24.4.2(h)	NEW	N/A	N/A	NA
24.4.2(i)	NEW	N/A	N/A	MTCS is specific to network routing controls.
24.4.2(j)	INCLUDED	A.9.1.2 Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	NA
24.4.2(k)	INCLUDED	A.9.4.1 Information access restriction	To prevent unauthorized access to systems and applications.	MTCS is specific to access restriction to virtualised layer.
24.4.2(l)	NEW	N/A	N/A	MTCS is specific to implementation of multi-factor to restrict access to hypervisor.
24.4.2(m)	NEW	N/A	N/A	MTCS is specific on installation and configuration of firewalls between wireless networks and cloud infrastructure.

24.4.2(n)	NEW	N/A	N/A	MTCS control requirement is specific to edge nodes in CSP to be safeguarded with secure protocols.
24.4.3 Level 2 requirements				
24.4.3(a)	NEW	N/A	N/A	ISO 27K did not specify restrictions in inbound/ outbound traffic between network hosting.
24.4.3(b)	NEW	N/A	N/A	ISO 27K did not specify to limit unsecured traffic to unsecure zone of the Cloud Service Delivery and Cloud service management network.
24.4.3(c)	INCLUDED	A.13.1.1 Network controls	Networks should be managed and controlled to protect information in systems and applications.	NA
24.4.3(d)	NEW	N/A	N/A	ISO 27K did not specify implementation of stateful inspection.
24.4.3(e)	NEW	N/A	N/A	ISO 27K did not specify internal IP Address disclosure.
24.4.3(f)	INCLUDED	A.13.1.3 Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	ISO27K covers this on a high level
24.4.4 Level 3 requirements				
24.4.4	NEW	N/A	N/A	MTCS is specific on installation and configuration of firewalls between wireless networks and cloud infrastructure.
24.5 Virtualisation				
24.5.1 General				
Control Objective	INCREMENTAL	A.6.1.5 Information security in project management	6.1.5 Information security in project management	ISO 27K did not specify how the Cloud Service Provider shall assess and manage information security risk during deployment of cloud technology. But ISO27K says that an information security risk assessment should be conducted at an early stage of the project to identify necessary controls;
24.5.2 Level 1 requirements				

24.5.2(a)	INCLUDED	A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	ISO27k covers risk management at a high level
24.5.2(b)	INCLUDED	A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	ISO27k covers risk management at a high level
24.5.2(c)	INCLUDED	A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	ISO 27K covers encryption at a high level
24.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
24.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
24.6 Storage area networks (SAN)				
24.6.1 General				
Control Objective	INCREMENTAL	A.9.1.2 Access to networks and network services A.13.1 Network security management	Users should only be provided with access to the network and network services that they have been specifically authorized to use. To ensure the protection of information in networks and its supporting information processing facilities.	See clauses below
24.6.2 Level 1 requirements				
24.6.2(a)	INCLUDED	A.9.1.2 Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	NA
24.6.2(b)	INCLUDED	A.13.1 Network security management	To ensure the protection of information in networks and its supporting information processing facilities.	NA
24.6.3 Level 2 requirements				

24.6.3(a)	INCLUDED	A.9.1.2 Access to networks and network services A.13.1 Network security management A.6.2.1 Mobile device policy	Users should only be provided with access to the network and network services that they have been specifically authorized to use. To ensure the protection of information in networks and its supporting information processing facilities. A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	NA
24.6.3(b)	NEW	N/A	N/A	ISO 27K did not mentioned that port controls to restrict the functionality of each port.
24.6.3(c)	INCREMENTAL	A.14.1.3 Protecting application services transactions A.10.1.2 Key management	Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	ISO27K states the below requirements A.14.1.3 d) protocols used to communicate between all involved parties are secured; A.14.1.3 f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process. A.10.1.2 b) issuing and obtaining public key certificates;
24.6.3(d)	NEW	N/A	N/A	ISO 27K did not mentioned that storage devices can only respond to request from authorised devices
24.6.3(e)	NEW	N/A	N/A	ISO 27K did not mentioned automatic replication.
24.6.4 Level 3 requirements				
24.6.4(a)	NEW	N/A	N/A	ISO 27K did not mentioned hard zones configured in the FC switch.

24.6.4(b)	NEW	N/A	N/A	ISO 27K did not mentioned Logical Unit Numbers (LUN) masking.
24.6.4(c)	NEW	N/A	N/A	ISO 27K did not mentioned that encryption will be provided to protect data at rest and in transit between storage devices.
24.6.4(d)	NEW	N/A	N/A	ISO 27K did not mentioned that customers have the options to maintain control of the encryption keys.
24.7 Data segregation				
24.7.1 General				
Control Objective	INCREMENTAL	A.9.4.1 Information access restriction	Access to information and application system functions should be restricted in accordance with the access control policy.	
24.7.2 Level 1 requirements **No applicable Level 1 controls**				
24.7.3 Level 2 requirements				
24.7.3(a)	INCREMENTAL	A.9.1.1 Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	ISO 27K did not covered logical segregation for logs and Encryption keys.
24.7.3(b)	INCLUDED	A.14.1.3 Protecting application services transactions	Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	NA
24.7.4 Level 3 requirements				
24.7.4(a)	INCLUDED	A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	NA
24.7.4(b)	NEW	N/A	N/A	ISO 27K did not mentioned that backups are segregated by cloud service customer.

<End of Gap Analysis Report>