INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

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

For cross-certification from ISO/IEC 27001:2005 to MTCS SS

December 2014

Revision History

Revision Date	Version	Updated by	Description
February 2014	Version 1.0	IDA	Initial release
December 2014	Version 1.1	IDA	Corrective or editorial revisions

Disclaimer

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

Copyright © 2014 Info-Communication Development Authority of Singapore. All rights reserved.

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

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

The experts of the Working Group are affiliated with:

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

The Multi-Tiered Cloud Security cross-certification Focus Group on ISO/IEC 27001:2005 to MTCS SS was appointed by IDA to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

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

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

Contents

1 Normative References

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

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

- **ISO/IEC 27001:2005** *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 27001:2005 benefits entities in allowing them to demonstrate commitment and compliance via the adoption of this standard.

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

2 Purpose of Document

This Gap Analysis Report is the first report in the set of three (3) documents to support cross certification between ISO/IEC 27001:2005 and MTCS SS. The purpose of each document is described in the diagram below.

Gap Analysis Report	Implementation Guideline Report	Audit Checklist Report
The purpose of the Gap Analysis Report is to provide an overview of the differences between the requirements listed in MTCS SS and the ISO/IEC 27001:2005 Standard. The information provided in this document aims to assist entities that are ISO/IEC 27001:2005 certified to adopt MTCS SS. Cloud Service Providers that are ISO/IEC 27001:2005 certified will have to comply with the requirements stated in MTCS SS that are currently omitted in ISO/IEC 27001:2005.	The purpose of the Implementation Guideline Report is meant to assist Cloud Service Providers that are ISO/IEC 27001:2005 certified to implement MTCS SS. The guidelines in the report are generic and need to be tailored to each Cloud Service Provider's specific requirements.	The purpose of the Audit Checklist Report is to guide Auditors including internal audit function, MTCS SS Certification Bodies and external audit bodies in understanding additional requirements beyond ISO/IEC 27001:2005. From the Cloud Service Providers' perspective, this document serves as a general guide for these providers to understand the scope covered in the MTCS SS certification audit when the scope of ISO/IEC 27001:2005 audit overlaps with scope of MTCS SS audit.

3 Intended Audience

This Gap Analysis Report is intended for Cloud Service Providers that are ISO/IEC 27001:2005 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 27001:2005.

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

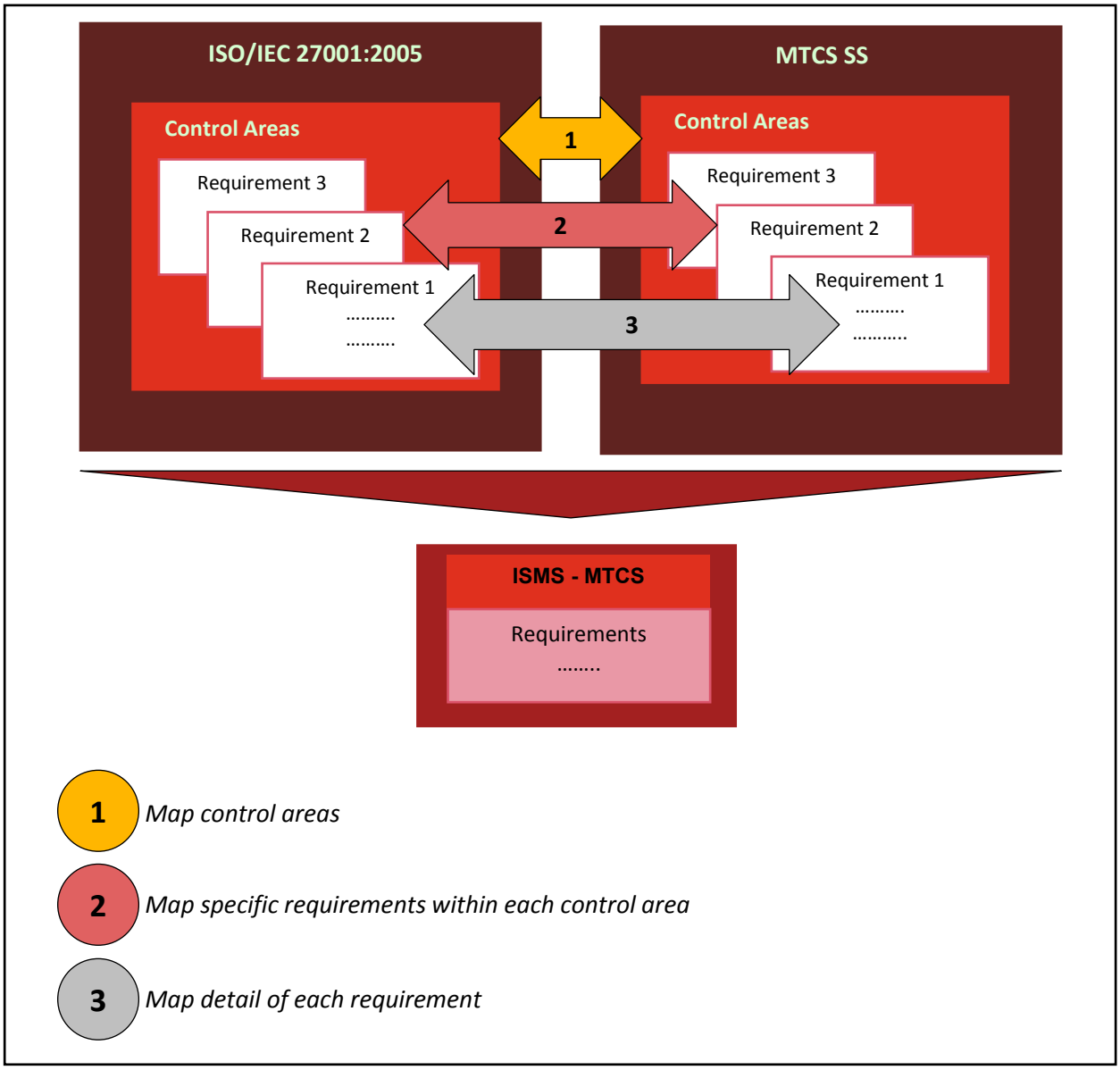
5 Terms and Definitions

ISMS-related terms used in this report are defined in ISO/IEC 27001:2005, 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 27001:2005 certified to adopt MTCS SS, requirements listed in ISO/IEC 27001:2005 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 27001:2005 categorised as follows:

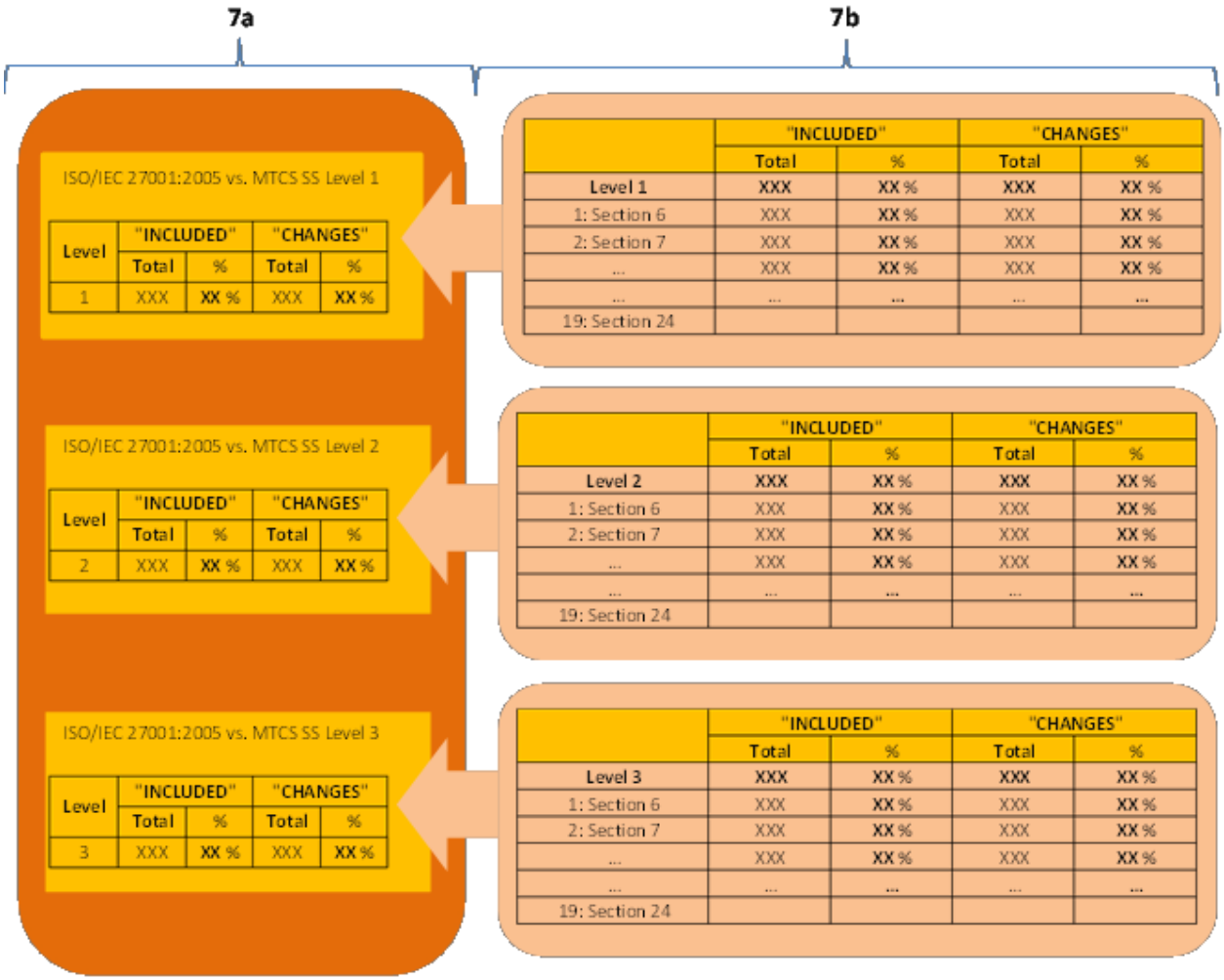
a. Summary by Levels in MTCS SS certification (Levels 1, 2 and 3)

Section 7.1 summarises the total gaps identified for ISO/IEC 27001:2005 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 27001:2005 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:



Cloud Service Providers that are ISO/IEC 27001:2005 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 27001:2005
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 27001:2005. In general, the requirements are classified as "INCREMENTAL" if the required enhancements on the existing ISO/IEC 27001:2005 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 27001:2005. 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 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 27001:2005.
- Yellow denotes >= 20% and < 50% MTCS SS controls included in ISO/IEC 27001:2005.
- Red denotes < 20% MTCS SS controls included in ISO/IEC 27001:2005.

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 27001:2005 Standard as grouped by MTCS SS certification Levels 1, 2 and 3. Cloud Service Providers that are ISO/IEC 27001:2005 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 27001:2005. Cloud Service Providers looking to be cross certified to MTCS SS Level 1 can refer to this table for total requirements applicable to this level:

Level	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 1	296	134	**45%**	162	**55%**	125	**42%**	37	**13%**

The table below provides a high level summary of the differences between MTCS SS Level 2 and ISO/IEC 27001:2005. Cloud Service Providers looking to be cross certified to MTCS SS Level 2 can refer to this table for total requirements applicable to this level. Note that the total clauses of 449 comprises of the 296 clauses in Level 1 and in addition, 153 unique Level 2 clauses.

Level	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 2	449	179	**40%**	270	**60%**	211	**47%**	59	**13%**

The table below provides a high level summary of the differences between MTCS SS Level 3 and ISO/IEC 27001:2005. Cloud Service Providers looking to be cross certified to MTCS SS Level 3 can refer to this table for total requirements applicable to this level. Note that the total clauses of 535 comprises of the 449 clauses in Level 2 and in addition, 86 unique Level 3 clauses.

Level	Total Clauses	"INCLUDED"		"CHANGES" = "INCREMENTAL" + "NEW"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Level 3	535	196	**37%**	339	**63%**	251	**47%**	88	**16%**

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 27001:2005 Standard by Control Areas in MTCS SS Levels 1, 2 and 3. Cloud Service Providers that are ISO/IEC 27001:2005 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 27001:2005[1]:

Sections	Total Clauses	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	32	22	**69%**	10	**31%**	10	**31%**	0	**0%**
Section 7	10	9	**90%**	1	**10%**	1	**10%**	0	**0%**
Section 8	8	5	**63%**	3	**38%**	3	**38%**	0	**0%**
Section 9	7	5	**71%**	2	**29%**	1	**14%**	1	**14%**
Section 10	18	8	**44%**	10	**56%**	5	**28%**	5	**28%**
Section 11	17	5	**29%**	12	**71%**	10	**59%**	2	**12%**
Section 12	9	5	**56%**	4	**44%**	3	**33%**	1	**11%**
Section 13	13	10	**77%**	3	**23%**	3	**23%**	0	**0%**
Section 14	23	7	**30%**	16	**70%**	16	**70%**	0	**0%**
Section 15	6	1	**17%**	5	**83%**	3	**50%**	2	**33%**
Section 16	15	7	**47%**	8	**53%**	5	**33%**	3	**20%**
Section 17	14	2	**14%**	12	**86%**	10	**71%**	2	**14%**
Section 18	27	11	**41%**	16	**59%**	13	**48%**	3	**11%**
Section 19	3	1	**33%**	2	**67%**	2	**67%**	0	**0%**
Section 20	5	2	**40%**	3	**60%**	3	**60%**	0	**0%**
Section 21	11	8	**73%**	3	**27%**	3	**27%**	0	**0%**
Section 22	34	10	**29%**	24	**71%**	16	**47%**	8	**24%**
Section 23	23	6	**26%**	17	**74%**	11	**48%**	6	**26%**
Section 24	21	10	**48%**	11	**52%**	7	**33%**	4	**19%**
Level 1	**296**	**134**	**45%**	**162**	**55%**	**125**	**42%**	**37**	**13%**

[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 27001:2005[1]:

Sections	Total Clauses	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	40	27	**68%**	13	**33%**	12	**30%**	1	**3%**
Section 7	20	12	**60%**	8	**40%**	8	**40%**	0	**0%**
Section 8	16	8	**50%**	8	**50%**	8	**50%**	0	**0%**
Section 9	10	5	**50%**	5	**50%**	4	**40%**	1	**10%**
Section 10	22	9	**41%**	13	**59%**	7	**32%**	6	**27%**
Section 11	24	7	**29%**	17	**71%**	15	**63%**	2	**8%**
Section 12	33	13	**39%**	20	**61%**	17	**52%**	3	**9%**
Section 13	22	14	**64%**	8	**36%**	7	**32%**	1	**5%**
Section 14	26	7	**27%**	19	**73%**	18	**69%**	1	**4%**
Section 15	8	1	**13%**	7	**88%**	5	**63%**	2	**25%**
Section 16	21	8	**38%**	13	**62%**	8	**38%**	5	**24%**
Section 17	22	2	**9%**	20	**91%**	18	**82%**	2	**9%**
Section 18	32	13	**41%**	19	**59%**	15	**47%**	4	**13%**
Section 19	9	3	**33%**	6	**67%**	6	**67%**	0	**0%**
Section 20	12	3	**25%**	9	**75%**	7	**58%**	2	**17%**
Section 21	13	10	**77%**	3	**23%**	3	**23%**	0	**0%**
Section 22	50	12	**24%**	38	**76%**	28	**56%**	10	**20%**
Section 23	32	8	**25%**	24	**75%**	13	**41%**	11	**34%**
Section 24	37	17	**46%**	20	**54%**	12	**32%**	8	**22%**
Level 2	**449**	**179**	**40%**	**270**	**60%**	**211**	**47%**	**59**	**13%**

[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 27001:2005[1]:

Sections	Total Clauses	"INCLUDED"		"CHANGES"		"INCREMENTAL"		"NEW"	
		Total	%	Total	%	Total	%	Total	%
Section 6	41	28	**68%**	13	**32%**	12	**29%**	1	**2%**
Section 7	24	13	**54%**	11	**46%**	11	**46%**	0	**0%**
Section 8	18	8	**44%**	10	**56%**	10	**56%**	0	**0%**
Section 9	17	6	**35%**	11	**65%**	7	**41%**	4	**24%**
Section 10	24	9	**38%**	15	**63%**	8	**33%**	7	**29%**
Section 11	29	8	**28%**	21	**72%**	16	**55%**	5	**17%**
Section 12	38	14	**37%**	24	**63%**	19	**50%**	5	**13%**
Section 13	27	17	**63%**	10	**37%**	7	**26%**	3	**11%**
Section 14	31	7	**23%**	24	**77%**	21	**68%**	3	**10%**
Section 15	11	1	**9%**	10	**91%**	7	**64%**	3	**27%**
Section 16	23	8	**35%**	15	**65%**	8	**35%**	7	**30%**
Section 17	23	2	**9%**	21	**91%**	19	**83%**	2	**9%**
Section 18	32	13	**41%**	19	**59%**	15	**47%**	4	**13%**
Section 19	25	3	**12%**	22	**88%**	18	**72%**	4	**16%**
Section 20	14	3	**21%**	11	**79%**	8	**57%**	3	**21%**
Section 21	20	14	**70%**	6	**30%**	6	**30%**	0	**0%**
Section 22	56	13	**23%**	43	**77%**	33	**59%**	10	**18%**
Section 23	34	9	**26%**	25	**74%**	13	**38%**	12	**35%**
Section 24	48	20	**42%**	28	**58%**	13	**27%**	15	**31%**
Level 3	**535**	**196**	**37%**	**339**	**63%**	**251**	**47%**	**88**	**16%**

[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 27001:2005 clauses" specifies the clauses that are currently stated in the ISO/IEC 27001:2005 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 27001:2005 subclauses" specifies the subclauses that are currently stated in the ISO/IEC 27001:2005 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 27001:2005 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.

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

MTCS SS has several requirements that are mutually exclusive across Levels 1, 2 and 3. Cloud Service Providers should note that they can only comply with requirements for the specific level in areas involving frequency of activities. For example, in MTCS SS Clause 15.1 'Vulnerability scanning', Cloud Service Providers have to conduct vulnerability scanning more frequently 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 27001:2005 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6 Information security management				
6.1 Information security management system (ISMS)				
6.1.1 General				
Control Objective	INCLUDED	4.0 ISMS 5.0 Management Responsibility 6.0 Internal ISMS audits A.5 Security policy A.8 Human resources security A.10 Communications and operations management A.11 Access control A.12 Information systems acquisition, development and maintenance A.15 Compliance	4.0 for general requirements including documentations 5.0 for management approval and communications 6.0 for audit requirements	N.A
6.1.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.1.2(a)	INCLUDED	4.2.1 Establish the ISMS A.9 Physical and environmental security A.11 Access Control A.12 Information systems acquisition, development and maintenance	4.2.1(a) Definition of scope and boundaries 4.2.1(b) Define ISMS policy 4.2.1(c) Define risk assessment approach 4.2.1(d) Identify risks - assets, threats, vulnerabilities, impacts that losses of confidentiality, integrity and availability may have on assets 4.2.1(e) Analyze and evaluate assets 4.2.1(f) Identify and evaluate options for treatment of risks 4.2.1(g) Select control objectives and treatment of risks 4.2.2 Implement and operate the ISMS - risk treatment plan	N.A
6.1.2(b)	INCLUDED	4.2.1 Establish the ISMS	4.2.1(b) Define ISMS policy 4.2.1(c) Define risk assessment approach 4.2.1(d) Identify risks 4.2.1(e) Analyze and evaluate assets 4.2.1(f) Identify and evaluate options for treatment of risks 4.2.1(g) Select control objectives and treatment of risks 4.2.2 Implement and operate the ISMS - risk treatment plan	Details on "cloud environment" not mentioned but traditional ISMS risk management in ISO/IEC 27001:2005 would sufficiently cover cloud-specific risk management function in 6.1.2(b).
6.1.2(c)	INCLUDED	4.2.1 Establish the ISMS 4.3.1 General 5.1 Management commitment A.5.1 Information security policy	4.2.1(b) Define ISMS policy 4.3.1(a) documented statements of the ISMS policy and objectives 5.1(a) establishing an ISMS policy A.5.1 Information security policy (all)	N.A
6.1.2(d)	INCLUDED	5.1 Management commitment A.8.1 Prior to employment	5.1(c) establishing roles and responsibilities for information security A.8.1.1 Roles and responsibilities	N.A
6.1.2(e)	INCREMENTAL	4.2.1 Establish the ISMS A.8 Human Resource security	4.2.1(f) Identify and evaluate options for the treatment of risks	Controls to mitigate risks mentioned in general but not specific for authorised insiders.
6.1.2(f)	INCLUDED	A.10 Communications and operations management (all)	A.10 Communications and operations management (all)	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.1.2(g)	INCLUDED	A.11 Access control (all)	A.11 Access control (all)	N.A
6.1.2(h)	INCLUDED	A.12 Information systems acquisition, development and maintenance (all)	A.12 Information systems acquisition, development and maintenance (all)	N.A
6.1.2(i)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.1(h) Obtain management approval of the proposed residual risks 4.2.1(i) Obtain management authorization to implement and operate the ISMS 4.2.1(j) Prepare a Statement of Applicability	Controls to mitigate risks mentioned in general but not specific for cloud computing.
6.1.2(j)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	No mention of "virtualisation", although generic security controls are mentioned. Additional security measures required for virtualisation (e.g., hypervisor) is not mentioned.
6.1.3 Level 2 requirements				
6.1.3(a)	INCLUDED	A.15.1 Compliance with legal requirements	A.15.1.4 Data protection and privacy of personal information	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.1.3(b)	INCLUDED	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS 4.3.1 General	4.2.2(d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3(c)) 4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 4.2.3(c) Measure the effectiveness of controls to verify that security requirements have been met. 4.3.1(g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3(c))	N.A
6.1.4 Level 3 requirements				
6.1.4(a)	INCLUDED	N.A	N.A	The assumption is that the interested CSPs are already ISO/IEC 27001:2005 certified.
6.2 Management of information security				
6.2.1 General				
Control Objective	INCLUDED	4.0 ISMS 5.0 Management responsibility A.5 Security policy A.6 Organization of information security A.8 Human resources security A.11 Access Control	N.A	N.A
6.2.2 Level 1 requirements				
6.2.2(a)	INCLUDED	5.1 Management commitment A.8.1 Prior to employment	5.1(c) establishing roles and responsibilities for information security A.8.1.1 Roles and responsibilities	N.A
6.2.2(b)	INCLUDED	A.6.1 Internal organization	A.6.1.2 Information security coordination	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.2.2(c)	INCLUDED	4.2.1 Establish the ISMS A.5.1 Information security policy A.6.1 Internal organization	4.2.1(b1) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security A.5.1.1 Information security policy document A.6.1.1 Management commitment to information security	N.A
6.2.2(d)	INCLUDED	A.6.2 External parties A.8.1 Prior to employment A.8.2 During employment A.10.2 Third party service delivery management A.10.8 Exchange of information A.11 Access Control (all)	A.6.2.1 Identification of risks related to external parties A.6.2.3 Addressing security in third party agreements A.8.1.3 Terms and conditions of employment A.8.2.1 Management responsibilities A.8.2.2 Information security awareness, education and training A.10.2.1 Service delivery A.10.2.2 Monitoring and review of third party services A.10.8.2 Exchange agreements A.11 Access Control (all)	N.A
6.2.3 Level 2 requirements				
6.2.3(a)	INCLUDED	5.1 Management commitment 5.2.1 Provision of resources 5.2.2 Training, awareness and competence	5.1(b) ensuring that ISMS objectives and plans are established 5.1(d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement 5.2.1(b) ensure that information security procedures support the business requirements 5.2.1(c) identify and address legal and regulatory requirements and contractual security obligations 5.2.2(b) providing training or taking other actions (e.g., employing competent personnel) to satisfy these needs	N.A
6.2.3(b)	INCLUDED	A.6.1 Internal organization	A.6.1.4 Authorization process for information processing facilities	N.A
6.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.3 Management oversight of information security				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.3.1 General				
Control Objective	INCLUDED	5.0 Management responsibility 6.0 Internal ISMS audits 7.0 Management review of the ISMS A.6 Organization of information security	N.A	N.A
6.3.2 Level 1 requirements				
6.3.2(a)	INCLUDED	5.1 Management commitment	5.1 Management commitment (all)	N.A
6.3.2(b)	INCLUDED	5.1 Management commitment5.2 Resource management6.0 Internal ISMS audits7.2 Review inputA.6.1 Internal organization	5.1(e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1) 5.1(h) conducting management reviews of the ISMS (see 7) 5.2.1 Provision of resources (all) 6.0 Internal ISMS audits (all) 7.2(d) status of preventive and corrective actions 7.2(f) results from effectiveness measurements 7.2(i) recommendations for improvement A.6.1.1 Management commitment to information security	N.A
6.3.2(c)	INCLUDED	5.1 Management commitment 7.2 Review input 7.3 Review output	5.1(b) ensuring that ISMS objectives and plans are established 5.1(d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement 5.1(f) deciding the criteria for accepting risks and the acceptable levels of risk 7.2 Review input (all) 7.3 Review output (all)	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
6.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.4 Information security policy				
6.4.1 General				
Control Objective	INCLUDED	4.0 ISMS 5.0 Management responsibility A.5 Security policy A.8 Human resources security	N.A	N.A
6.4.2 Level 1 requirements				
6.4.2(a)	INCLUDED	4.2.1 Establish the ISMS 5.1 Management commitment A.5.1 Information security policy	4.2.1(b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology 5.1(a) establishing an ISMS policy A.5.1.1 Information security policy document	N.A
6.4.2(b)	INCREMENTAL	4.2.2 Implement and operate the ISMS 5.1 Management commitment A.8.1 Prior to employment	4.2.2(b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities 5.1(c) establishing roles and responsibilities for information security A.8.1.1 Roles and responsibilities	Strategic plan was not explicitly mentioned. However, components of a possible strategic plan can be observed. Other requirements on strategic plan stated in ISO risk assessment standards are not fully met by ISO/IEC 27001:2005.
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 Review of information security policy				
6.5 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCLUDED	4.0 ISMS 5.0 Management responsibility 7.0 Management review of the ISMS A.5 Security policy	N.A	N.A
6.5.2 Level 1 requirements				
6.5.2(a)	INCLUDED	4.2.3 Monitor and review the ISMS 5.1 Management commitment 7.1 General A.5.1 Information security policy	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 5.1(h) conducting management reviews of the ISMS (see 7) 7.1 General (all) A.5.1.2 Review of the information security policy	N.A
6.5.3 Level 2 requirements				
6.5.3(a)	INCLUDED	4.2.3 Monitor and review the ISMS 5.1 Management commitment 7.1 General A.5.1 Information security policy	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 5.1(h) conducting management reviews of the ISMS (see 7) 7.1 General (all) A.5.1.2 Review of the information security policy	N.A
6.5.4 Level 3 requirements **The requirement is the same as that in Level 2.**				
6.6 Information security audits				
6.6.1 General				
Control Objective	INCLUDED	4.0 ISMS 6.0 Internal ISMS audits A.15 Compliance	N.A	N.A
6.6.2 Level 1 requirements				
6.6.2(a)	INCREMENTAL	4.2.3 Monitor and review the ISMS 6 Internal ISMS audits	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 6 Internal ISMS audits (all)	ISO/IEC 27001:2005 Sections 4.2.3 and 6.0 mention of undertaking regular reviews of the effectiveness of the ISMS, but no mention of a formal audit committee.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.6.2(b)	INCREMENTAL	6 Internal ISMS audits A.15 Information systems audit considerations A.10 Communications and operations management	6 Internal ISMS audits A.15.3 Information systems audit considerations A.10.2.2 Monitoring and review of third party services	Planning an ISMS audit in general, but no specific mention of approval process or audit committee.
6.6.2(c)	INCREMENTAL	4.2.3 Monitor and review the ISMS 6 Internal ISMS audits	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 4.2.3(e) Conduct internal ISMS audits at planned intervals (see 6) 6 Internal ISMS audits	Frequency of such audits not mentioned.
6.6.2(d)	INCLUDED	4.2.3 Monitor and review the ISMS 6 Internal ISMS audits	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 6 Internal ISMS audits	N.A
6.6.2(e)	INCLUDED	A.15.3 Information systems audit considerations	A.15.3.2 Protection of information systems audit tools	N.A
6.6.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
6.6.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.7 Information security liaisons (ISL)				
6.7.1 General				
Control Objective	INCLUDED	5.0 Management responsibility A.6 Organization of information security A.8 Human resources security	N.A	N.A
6.7.2 Level 1 requirements				
6.7.2(a)	INCLUDED	A.6.1 Internal organization	A.6.1.6 Contact with authorities	N.A
6.7.2(b)	INCLUDED	A.6.1 Internal organization	A.6.1.7 Contact with special interest groups	N.A
6.7.2(c)	INCLUDED	A.6.1 Internal organization	A.6.1.7 Contact with special interest groups	ISO/IEC 27001:2005 Section A.6.1.7 mentions "appropriate contacts" but not explicitly security bulletins and alerts.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.7.2(d)	INCREMENTAL	5.2 Resource management A.8.2 During employment	5.2.2 Training, awareness and competence A.8.2.2 Information security awareness, education and training	Awareness and training is present but specific topic of external risk development not mentioned.
6.7.3 Level 2 requirements				
6.7.3(a)	NEW	N.A	N.A	ISO/IEC 27001:2005 Sections A.6.1.6 and A.6.1.7 mention requirement on ISL but details on being available for contact by customers are not mentioned.
6.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
6.8 Acceptable Usage				
6.8 General				
Control Objective	INCLUDED	A.7 Asset management A.10 Communications and operations management	A.7 Asset management A.10 Communications and operations management	N.A
6.8.2 Level 1 requirements				
6.8.2(a)	INCREMENTAL	A.7.1 Responsibility for assets	A.7.1.3 Acceptable use of assets	Definition of rules for acceptable usage was mentioned but not details about approval process by authorised parties.
6.8.2(b)	INCREMENTAL	A.7.1 Responsibility for assets	A.7.1.3 Acceptable use of assets	Definition of rules for acceptable usage was mentioned but not details about specific authentication technology, service, device or company-approved product.
6.8.2(c)	INCLUDED	A.7.1 Responsibility for assets	A.7.1.3 Acceptable use of assets	N.A
6.8.3 Level 2 requirements				
6.8.3(a)	INCREMENTAL	A.7.1 Responsibility for assets A.7.2 Information classification	A.7.1.3 Acceptable use of assets A.7.2.2 Information labeling and handling	Definition of rules for acceptable usage was mentioned but not details about network locations, services, devices and company-approved products.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
6.8.3(b)	INCREMENTAL	A.10.7 Media handling A.11.4 Network Access Control	A.10.7.3 Information handling procedures A.11.4 Network Access Control (all)	Details about handling information are mentioned in ISO/IEC 27001:2005 Section A.10.7.3 and network technologies/controls in ISO/IEC 27001:2005 Section A.11.4 but explicit authorisation or approval process was not mentioned, including access via gateways and VPNs.
6.8.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
7 Human resources				
7.1 Background screening				
7.1.1 General				
Control Objective	INCLUDED	A.8 Human resources security	N.A	N.A
7.1.2 Level 1 requirements				
7.1.2(a)	INCLUDED	A.8.1 Prior to employment	A.8.1 Prior to employment (all)	N.A
7.1.2(b)	INCREMENTAL	A.8.1 Prior to employment	A.8.1.2 Screening A.8.1.3 Terms and conditions of employment	Components of background checks such as identity verification, character references, CV verification, criminal and credit checks not explicitly mentioned.
7.1.3 Level 2 requirements				
7.1.3(a)	INCREMENTAL	A.8.1 Prior to employment	A.8.1.2 Screening	Background check frequency not mentioned in ISO/IEC 27001:2005.
7.1.4 Level 3 requirements				
7.1.4(a)	INCREMENTAL	A.8.1 Prior to employment	A.8.1.2 Screening	Background check frequency not mentioned in ISO/IEC 27001:2005.
7.2 Continuous personnel evaluation				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
7.2.1 General				
Control Objective	INCLUDED	5.0 Management responsibility A.6 Organization of information security A.8 Human resources security A.10 Communications and operations management A.11 Access control	N.A	N.A
7.2.2 Level 1 requirements **No applicable Level 1 controls.**				
7.2.3 Level 2 requirements				
7.2.3(a)	INCREMENTAL	5.2.2 Training, awareness and competence A.8.1 Prior to employment A.8.2 During employment A.11.2 User access management	5.2.2(a) determining the necessary competencies for personnel performing work effecting the ISMS 5.2.2(c) evaluating the effectiveness of the actions taken 5.2.2(d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3) A.8.1.2 Screening A.8.2.2 Information security awareness, education and training A.11.2.4 Review of user access rights	Evaluation frequency not mentioned in ISO/IEC 27001:2005.
7.2.3(b)	INCREMENTAL	5.2.2 Training, awareness and competence A.6.2 External parties A.8.1 Prior to employment A.8.2 During employment A.8.3 Termination or change of employment A.11.2 User access management	5.2.2(a) determining the necessary competencies for personnel performing work effecting the ISMS 5.2.2(c) evaluating the effectiveness of the actions taken 5.2.2(d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3) A.6.2.3 Addressing security in third party agreements A.8.1.2 Screening A.8.1.3 Terms and conditions of employment A.8.2.2 Information security awareness, education and training A.8.3 Termination or change of employment (all) A.11.2.4 Review of user access rights	Evaluation coverage not mentioned in ISO/IEC 27001:2005.
7.2.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
7.2.4(a)	INCREMENTAL	5.2.2 Training, awareness and competence A.8.1 Prior to employment A.8.2 During employment A.11.2 User access management	5.2.2(a) determining the necessary competencies for personnel performing work effecting the ISMS 5.2.2(c) evaluating the effectiveness of the actions taken 5.2.2(d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3) A.8.1.2 Screening A.8.2.2 Information security awareness, education and training A.11.2.4 Review of user access rights	Evaluation frequency not mentioned in ISO/IEC 27001:2005.
7.2.4(b)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use A.10.10.3 Protection of log information	N.A
7.3 Employment and contract terms and conditions				
7.3.1 General				
Control Objective	INCLUDED	A.8 Human resources security	N.A	N.A
7.3.2 Level 1 requirements				
7.3.2(a)	INCLUDED	A.8.2 During employment	A.8.2.1 Management responsibilities	N.A
7.3.2(b)	INCLUDED	A.8.1 Prior to employment	A.8.1.3 Terms and conditions of employment	N.A
7.3.2(c)	INCLUDED	A.8.3 Termination or change of employment	A.8.3.2 Return of assets A.8.3.3 Removal of access rights	N.A
7.3.2(d)	INCLUDED	A.8.1 Prior to employment	A.8.1.3 Terms and conditions of employment	Implicit acknowledgement from signing of employment contract.
7.3.3 Level 2 requirements				
7.3.3(a)	INCLUDED	A.8.3 Termination or change of employment	A.8.3.1 Termination responsibilities	N.A
7.3.3(b)	INCLUDED	A.8.3 Termination or change of employment	A.8.3 Termination or change of employment (all)	N.A
7.3.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
7.3.4(a)	INCREMENTAL	A.8.1 Prior to employment	A.8.1.3 Terms and conditions of employment	Implicit acknowledgement from signing of employment contract but of re-acknowledgement and re-acknowledge frequency was not mentioned.
7.4 Disciplinary process				
7.4.1 General				
Control Objective	INCLUDED	A.8 Human resources security	N.A	N.A
7.4.2 Level 1 requirements				
7.4.2(a)	INCLUDED	A.8.2 During employment	A.8.2.3 Disciplinary process	N.A
7.4.3 Level 2 requirements **The requirement is the same as that in Level 1.**				
7.4.4 Level 3 requirements **The requirement is the same as that in Level 2.**				
7.5 Asset returns				
7.5.1 General				
Control Objective	INCLUDED	A.8 Human resources security	N.A	N.A
7.5.2 Level 1 requirements				
7.5.2(a)	INCLUDED	A.8.3 Termination or change of employment	A.8.3.1 Termination responsibilities A.8.3.2 Return of assets	N.A
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 Information security training and awareness				
7.6.1 General				
Control Objective	INCREMENTAL	4.2 Establishing and managing the ISMS 5.2 Resource Management A.8 Human resources security A.15 Compliance	N.A	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
7.6.2 Level 1 requirements				
7.6.2(a)	INCLUDED	4.2.2 Implement and operate the ISMS5.2.2 Training, awareness and competenceA.8.2 During employment	4.2.2(e) Implement training and awareness programs (see 5.2.2) 5.2.2 Training, awareness and competence A.8.2.2 Information security awareness, education and training	N.A
7.6.2(b)	INCLUDED	4.2.2 Implement and operate the ISMS 5.2.2 Training, awareness and competence A.8.2 During employment A.13.1 Reporting information security events and weaknesses	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a)) 4.2.3(a) Execute monitoring and reviewing procedures 5.2.2 Training, awareness and competence A.8.2.2 Information security awareness, education and training A.13.1.1 Reporting information security events	N.A
7.6.3 Level 2 requirements				
7.6.3(a)	INCREMENTAL	4.2.2 Implement and operate the ISMS 5.2.2 Training, awareness and competence A.8.2 During employment	4.2.2(e) Implement training and awareness programs (see 5.2.2) 5.2.2 Training, awareness and competence A.8.2.2 Information security awareness, education and training	Awareness in general mentioned but specific topic about sensitive data in cloud environment was not mentioned.
7.6.3(b)	INCLUDED	4.2.2 Implement and operate the ISMS 5.2.2 Training, awareness and competence A.8.2 During employment	4.2.2(e) Implement training and awareness programs (see 5.2.2) 5.2.2 Training, awareness and competence A.8.2.2 Information security awareness, education and training	N.A
7.6.3(c)	INCREMENTAL	A.5.1 Information security policy A.15.1 Compliance with legal requirements	A.5.1.1 Information security policy document A.15.1.4 Data protection and privacy of personal information	Communication of information security policy mentioned but the communication of data protection policy though there are elements of data protection in ISO/IEC 27001:2005 Section A.15.1.4.
7.6.3(d)	INCREMENTAL	A.8.2 During employment	A.8.2.2 Information security awareness, education and training	Awareness in general but specific topic about personal data was not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
7.6.3(e)	INCREMENTAL	4.2.2 Implement and operate the ISMS 5.2.2 Training, awareness and competence A.8.2 During employment	4.2.2(e) Implement training and awareness programs (see 5.2.2) 5.2.2 Training, awareness and competence A.8.2.2 Information security awareness, education and training	Computer Misuse Act is not explicitly mentioned.
7.6.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8 Risk management				
8.1 Risk management program				
8.1.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 7.0 Management review of the ISMS 8.0 ISMS improvement A.6 Organization of information security	N.A	Cloud specific programs are not mentioned.
8.1.2 Level 1 requirements				
8.1.2(a)	INCLUDED	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 4.3.1 General 7.3 Review output	4.2.1(c) Define the risk assessment methodology of the organization 4.2.3(d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks 4.3.1(d) documentation on the risk assessment methodology (see 4.2.1(c)) 4.3.1(e) the risk assessment report (see 4.2.1(c) to 4.2.1(g)) 7.3(b) Update of the risk assessment and risk treatment plan	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8.1.2(b)	INCLUDED	A.6.2 External parties 4.2.1 Establish the ISMS	A.6.2.1 Identification of risks related to external parties 4.2.1(d) Identify the risks	N.A
8.1.2(c)	INCLUDED	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 4.3.1 General 7.3 Review output	4.2.1(c) Define the risk assessment approach of the organization 4.2.3(d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks 4.3.1(d) a description of the risk assessment methodology (see 4.2.1(c)) 4.3.1(e) the risk assessment report (see 4.2.1(c) to 4.2.1(g)) 7.3(b) Update of the risk assessment and risk treatment plan	N.A
8.1.2(d)	INCLUDED	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS 4.3.1 General	4.2.1(e) Analyze and evaluate the risks 4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.1(j) Prepare a Statement of Applicability 4.2.2(a) Formulate a risk treatment plan 4.2.2(b) Implement the risk treatment plan 4.3.1(f) the risk treatment plan (see 4.2.2(b)) 7.3(b) Update of the risk assessment and risk treatment plan	N.A
8.1.2(e)	INCLUDED	8.1 Continual improvement 8.2 Corrective action 8.3 Preventive action	8.1 Continual improvement 8.2 Corrective action (all) 8.3 Preventive action (all)	While the preventive and corrective actions are not specific to the usage of cloud services, the requirements are sufficient to cover cloud computing at a high level.
8.1.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8.1.3(a)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 5.1 Management commitment	4.2.1(b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology 4.2.1(c) Define the risk assessment approach of the organization 4.2.1(e) Analyze and evaluate the risks. 4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.3(d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks 5.1(f) deciding the criteria for accepting risks and the acceptable levels of risk	Elements of risk assessment and risk acceptance are present but specific categories of risk criteria not mentioned.
8.1.4 Level 3 requirements				
8.1.4(a)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 7.0 Management review of the ISMS	4.2.1(e) Analyze and evaluate the risks 4.2.3(a) Execute monitoring and reviewing procedures 4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 7.1 General	Frequency of risk review is not mentioned and risk metrics is not explicitly mentioned to be included in the scope of the review.
8.2 Risk assessment				
8.2.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 7.0 Management review of the ISMS A.14 Business continuity management A.15 Compliance	N.A	Cloud specific risk assessment not mentioned.
8.2.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8.2.2(a)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 7.2 Review input A.14.1 Information security aspects of business continuity management	4.2.1(c) Define the risk assessment approach of the organization 4.2.1(d) Identify the risks 4.2.1(e) Analyze and evaluate the risks 4.2.3(h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3) 7.2(e) vulnerabilities or threats not adequately addressed in the previous risk assessment A.14.1.2 Business continuity and risk assessment	Cloud specific risk assessment on threat and vulnerability assessment and impact assessment not mentioned.
8.2.2(b)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 7.2 Review input A.14.1 Information security aspects of business continuity management	4.2.1(c) Define the risk assessment approach of the organization. 4.2.1(d) Identify the risks 4.2.1(e) Analyze and evaluate the risks 4.2.3(h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3) 7.2(e) vulnerabilities or threats not adequately addressed in the previous risk assessment A.14.1.2 Business continuity and risk assessment	General ISMS risk assessment elements mentioned but do not include cloud specific areas.
8.2.2(c)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 7.2 Review input A.14.1 Information security aspects of business continuity management	4.2.1(c) Define the risk assessment approach of the organization 4.2.1(d) Identify the risks 4.2.1(e) Analyze and evaluate the risks 4.2.1(h) Obtain management approval of the proposed residual risks 4.2.3(d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks 4.2.3(h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3) 7.2(e) vulnerabilities or threats not adequately addressed in the previous risk assessment A.14.1.2 Business continuity and risk assessment	General ISMS risk assessment elements mentioned but do not include risk categories.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8.2.3 Level 2 requirements				
8.2.3(a)	INCREMENTAL	A.15.1 Compliance with legal requirements	A.15.1.4 Data protection and privacy of personal information	Data protection elements are included in ISO/IEC 27001:2005 Section A.15.1.4 but its inclusion in risk assessment was not mentioned.
8.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
8.3 Risk management				
8.3.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility 7.0 Management review of the ISMS 8.0 ISMS improvement	N.A	N.A
8.3.2 Level 1 requirements **No applicable Level 1 controls.**				
8.3.3 Level 2 requirements				
8.3.3(a)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS 8.3 Preventive action	4.2.1(b4) establishes criteria against which risk will be evaluated (see 4.2.1(c)) 4.2.1(e) Analyze and evaluate the risks. 4.2.2(a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5) 8.3 Preventive action	Priorities for managing information security risks imply prioritizing material risks.
8.3.3(b)	INCLUDED	4.2.3 Monitor and review the ISMS 5.1 Management commitment	4.2.3(d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks 5.1(e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1) 5.1(h) conducting management reviews of the ISMS (see 7)	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8.3.3(c)	INCLUDED	4.2.1 Establish the ISMS 8.3 Preventive action	4.2.1(e) Analyze and evaluate the risks 8.3(a) identifying potential nonconformities and their causes 8.3(b) evaluating the need for action to prevent occurrence of nonconformities	N.A
8.3.3(d)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS	4.2.1(b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology 4.2.1(c) Define the risk assessment approach of the organization 4.2.2(a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities 4.2.2(b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities	Development of strategy not mentioned though the policy could contain specific strategies and the approach being part of a strategy.
8.3.3(e)	INCLUDED	4.2.3 Monitor and review the ISMS7.2 Review input	4.2.3(a5) determine whether the actions taken to resolve a breach of security were effective 4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 4.2.3(d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks 7.2(d) status of preventive and corrective actions 7.2(e) vulnerabilities or threats not adequately addressed in the previous risk assessment 7.2(f) results from effectiveness measurements	N.A
8.3.4 Level 3 requirements				
8.3.4(a)	INCREMENTAL	4.2.2 Implement and operate the ISMS	4.2.2(d) Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3(c))	Metrics for the measurement of effectiveness of controls was mentioned but not metrics for IT risk.
8.4 Risk register				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
8.4.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility	N.A	N.A
8.4.2 Level 1 requirements **No applicable Level 1 controls.**				
8.4.3 Level 2 requirements				
8.4.3(a)	INCREMENTAL	4.2.1 Establish the ISMS 4.3.1 General 4.3.2 Control of documents 5.1 Management commitment	4.2.1(b) establishes criteria against which risk will be evaluated (see 4.2.1c) 4.2.1(c2) Develop criteria for accepting risks and identify the acceptable levels of risk (see 5.1f) 4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(h) Obtain management approval of the proposed residual risks 4.3.1(e) the risk assessment report (see 4.2.1(c) to 4.2.1(g)) 4.3.2(a) approve documents for adequacy prior to issue 4.3.2(b) review and update documents as necessary and re-approve documents 5.1(f) deciding the criteria for accepting risks and the acceptable levels of risk	Priority levels, control strategies and resolution timeframe not mentioned. Usage of a risk register was not mentioned but a risk assessment report may contain the risk register.
8.4.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
9 Third party				
9.1 Third party due diligence				
9.1.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management	A.6.2 External parties (all) A.10.8.2 Exchange agreements	Details as stated in the MTCS SS requirement are not mentioned.
9.1.2 Level 1 requirements				
9.1.2(a)	INCREMENTAL	A.6.2 External parties A.10.8 Exchange of information	A.6.2 External parties (all) A.10.8.2 Exchange agreements	Identification and addressing of risks associated with third parties mentioned but not the specific criteria (e.g., viability, capability, track record).
9.1.2(b)	INCLUDED	A.6.2 External parties A.10.8 Exchange of information	A.6.2 External parties (all) A.10.8.2 Exchange agreements	Evaluation of compliance with MTCS is not included in ISO/IEC 27001:2005 as MTCS is new.
9.1.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
9.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
9.2 Identification of risks related to third parties				
9.2.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management	A.6.2 External parties (all) A.10.8.2 Exchange agreements	Details on risk management procedures and access to information systems and data as stated in the requirement are not mentioned.
9.2.2 Level 1 requirements				
9.2.2(a)	INCLUDED	A.6.2 External parties A.10.2 Third party service delivery management A.10.8 Exchange of information	A.6.2.1 Identification of risks related to external parties A.6.2.3 Addressing security in third party agreements A.10.2 Third party service delivery management (all) A.10.8.1 Information exchange policies and procedures A.10.8.2 Exchange agreements	N.A
9.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
9.2.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
9.2.4(a)	NEW	N.A	N.A	Risk Assessment is mentioned in general however details on Threat and Vulnerability Risk Assessment (TVRA) at the data centre is not mentioned.
9.2.4(b)	NEW	N.A	N.A	Requirement on remediation plan is included; however, specific requirement for remediation plan by third party service providers are not mentioned.
9.3 Third party agreement				
9.3.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management A. 8.1.3 Terms and conditions of employment	N.A	N.A
9.3.2 Level 1 requirements				
9.3.2(a)	INCLUDED	A.6.2 External parties A.10.2 Third party service delivery management A. 8.1.3 Terms and conditions of employment	A.6.2.3 Addressing security in third party agreement A.10.2.1 Service delivery A. 8.1.3 Terms and conditions of employment - As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and condition	N.A
9.3.3 Level 2 requirements				
9.3.3(a)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management A.8.1.3 Terms and conditions of employment	A.6.2.3 Addressing security in third party agreement A.10.2.1 Service delivery A.8.1.3 Terms and conditions of employment	Not all detailed attributes to be addressed are present in ISO/IEC 27001:2005.
9.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
9.4 Third party delivery management				
9.4.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	A.10 Communications and operations management A.14 Business continuity management A.15 Compliance	N.A	N.A
9.4.2 Level 1 requirements				
9.4.2(a)	INCLUDED	A.10.2 Third party service delivery management	A.10.2.1 Service delivery	N.A
9.4.2(b)	INCLUDED	A.10.2 Third party service delivery management	A.10.2.3 Managing changes to third party services	N.A
9.4.2(c)	NEW	N.A	N.A	Implementation of policies, procedures and controls is mentioned however the expectations on the extent of these components are not mentioned.
9.4.3 Level 2 requirements				
9.4.3(a)	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management	A.10.2.2 Monitoring and review of third party services A.10.2.3 Managing changes to third party services	Details as listed are not mentioned, but monitoring and review of third party services and monitoring of changes are mentioned in general.
9.4.3(b)	INCREMENTAL	A.15.1 Compliance with legal requirements	A.15.1.4 Data protection and privacy of personal information	Mentioned in general and not specific to CSP.
9.4.4 Level 3 requirements				
9.4.4(a)	NEW	N.A	N.A	The extent of diligence and care for the specific elements are not mentioned.
9.4.4(b)	INCLUDED	A.10.2 Third party service delivery management	A.10.2.2 Monitoring and review of third party services	N.A
9.4.4(c)	INCREMENTAL	A.10.2 Third party service delivery management	A.10.2.2 Monitoring and review of third party services	The establishment of process to monitor third party service delivery was not mentioned.
9.4.4(d)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2 Third party service delivery management (all)	ISO/IEC 27001:2005 does not mention onsite visits explicitly though monitoring is present.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
9.4.4(e)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1 Information security aspects of business continuity management (all)	Disaster recovery and contingency planning were not mentioned.

9.5 Legal and compliance

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
10 Legal and compliance				
10.1 Compliance with regulatory and contractual requirements				
10.1.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.6 Organization of information security A.15 Compliance	N.A	N.A
10.1.2 Level 1 requirements				
10.1.2(a)	INCLUDED	A.15.1 Compliance with legal requirements	A.15.1.1 Identification of applicable legislation	N.A
10.1.2(b)	NEW	N.A	N.A	Cloud specific requirements on cross-border movement and data transit were not mentioned.
10.1.2(c)	INCLUDED	A.15.1 Compliance with legal requirements	A.15.1.1 Identification of applicable legislation	N.A
10.1.2(d)	NEW	N.A	N.A	Cloud specific requirements on cross-border movement and data transit were not mentioned.
10.1.3 Level 2 requirements				
10.1.3(a)	INCREMENTAL	4.3.2 Control of documents A.15.1 Compliance with legal requirements	4.3.2(b) review and update documents as necessary and re-approve documents A.15.1.1 Identification of applicable legislation	Review and update of documentations mentioned. However, there was no explicit mention of having an approach and for each category of IS element.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
10.1.3(b)	INCLUDED	A.6.1 Internal organization A.15.1 Compliance with legal requirements	A.6.1.5 Confidentiality agreements A.15.1.4 Data protection and privacy of personal information	N.A
10.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
10.2 Compliance with policies and standards				
10.2.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility 6.0 Internal ISMS audits A.6 Organization of information security A.10 Communications and operations management A.15 Compliance	N.A	Cloud specific requirements not mentioned, but generic requirements are mentioned.
10.2.2 Level 1 requirements				
10.2.2(a)	INCREMENTAL	4.2.3 Monitor and review the ISMS 5.1 Management commitment 6 Internal ISMS audits A.6.1 Internal organization A.10.2 Third party service delivery management A.15.3 Information systems audit considerations	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 4.2.3(e) Conduct internal ISMS audits at planned intervals (see 6) 5.1(g) ensuring that internal ISMS audits are conducted (see 6) 6 Internal ISMS audits (all) A.6.1.8 Independent review of information security A.10.2.2 Monitoring and review of third party services A.15.3.1 Information systems audit controls	Review and audit for ISMS in general. Review and audit for cloud services may include additional elements.
10.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
10.2.3(a)	INCREMENTAL	4.2.3 Monitor and review the ISMS 5.1 Management commitment 6 Internal ISMS audits A.6.1 Internal organization A.10.2 Third party service delivery management A.15.3 Information systems audit considerations	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 4.2.3(e) Conduct internal ISMS audits at planned intervals (see 6) 5.1(g) ensuring that internal ISMS audits are conducted (see 6) 6 Internal ISMS audits (all) A.6.1.8 Independent review of information security A.10.2.2 Monitoring and review of third party services A.15.3.1 Information systems audit controls	Review and audit for ISMS in general. Review and audit for CSP may include additional elements.
10.2.4 Level 3 requirements				
10.2.4(a)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(b) ISMS policy established to align with the organization's strategic risk management	Compliance or some form of alignment mentioned for ISMS policy establishment but not at the internal audit level.
10.3 Prevention of misuse of cloud facilities				
10.3.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.7 Asset management A.8 Human resources security A.10 Communications and operations management	N.A	N.A
10.3.2 Level 1 requirements				
10.3.2(a)	INCREMENTAL	A.7.1 Responsibility for assets A.8.2 During employment	A.7.1.3 Acceptable use of assets A.8.2.2 Information security awareness, education and training	Awareness and acceptable usage are mentioned but they are not specific to the cloud environment.
10.3.2(b)	INCREMENTAL	A.8.2 During employment	A.8.2.2 Information security awareness, education and training	Awareness in general mentioned but not specific topics about the monitoring features/controls in place.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
10.3.2(c)	NEW	N.A	N.A	Specific requirement on log-on warning message or reminder on access policies and monitoring for accessing infrastructure or other privileged access are not mentioned.
10.3.2(d)	NEW	N.A	N.A	Monitoring to detect if the cloud infrastructure is being used as a platform to attack others (e.g., nefarious use of cloud computing services) is not mentioned.
10.3.2(e)	INCLUDED	A.6.2 External parties A.8.1 Prior to employment A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.8.1.3 Terms and conditions of employment A.10.2.1 Service delivery	Though not mentioned explicitly, policies and restrictions could already have been included in the corresponding clauses.
10.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
10.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
10.4 Use of compliant cryptography controls				
10.4.1 General				
Control Objective	INCREMENTAL	A.12 Information systems acquisition, development and maintenance A.15 Compliance A.12.3	N.A	N.A
10.4.2 Level 1 requirements				
10.4.2(a)	INCLUDED	A.12.3 Cryptographic controls A.8.1.3 Terms and conditions of employment	A.12.3.1 Policy on the use of cryptographic controls A.8.1.3 Terms and conditions of employment	Use of cryptographic controls mentioned but not the inclusion of cryptography controls and policies in relevant agreements.
10.4.2(b)	INCLUDED	A.15.1 Compliance with legal requirements	A.15.1 Compliance with legal requirements (all)	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
10.4.2(c)	NEW	N.A	N.A	No specific mention of knowledge and application of prevailing industry practices.
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 Third party compliance				
10.5.1 General				
Control Objective	INCLUDED	A.5 Security policy A.8 Human resources security A.10 Communications and operations management A.15 Compliance	N.A	N.A
10.5.2 Level 1 requirements				
10.5.2(a)	INCLUDED	A.5.1 Information security policy A.8.1 Prior to employment A.10.8 Exchange of information	A.5.1.1 Information security policy document A.8.1.1 Roles and responsibilities A.10.8.1 Information exchange policies and procedures	N.A
10.5.2(b)	INCLUDED	A.10.2 Third party service delivery management A.10.6 Network security management	A.10.2.1 Service delivery A.10.6.2 Security of network services	N.A
10.5.2(c)	INCLUDED	A.15.1 Compliance with legal requirements	A.15.1.4 Data protection and privacy of personal information	N.A
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 Continuous compliance monitoring				
10.6.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	A.10 Communications and operations management A.15 Compliance	A.15 states requirements on compliance with legal requirements, security policies and standards, technical, and information systems audit requirements	Real-time compliance monitoring mechanism is not mentioned.
10.6.2 Level 1 requirements				
10.6.2(a)	INCREMENTAL	A.15.2 Compliance with security policies and standards, and technical compliance	A.15.2.2 Technical compliance checking	Details on system configuration compliance reporting framework is not mentioned. Furthermore, details on the areas to be covered under configuration baselines and access matrices are not listed.
10.6.2(b)	INCREMENTAL	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use A.10.10.5 Fault logging	Making logs available for cloud users for continuous and real-time monitor compliance not mentioned.
10.6.3 Level 2 requirements				
10.6.3(a)	NEW	N.A	N.A	No mention of reporting requirements on system access.
10.6.4 Level 3 requirements				
10.6.4(a)	NEW	N.A	N.A	No mention of security monitoring platform for cloud users.

9.6 Incident management

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11 Incident management				
11.1 Information security incident response plan and procedure				
11.1.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility 8 ISMS improvement A.6 Organization of information security A.8 Human resources security A.10 Communications and operations management A.13 Information security incident management A.14 Business continuity management A.15 Compliance	N.A	N.A
11.1.2 Level 1 requirements				
11.1.2(a)	INCREMENTAL	4.2.2 Implement and operate the ISMS 5.1 Management commitment A.8.1 Prior to employment A.13.2 Management of information security incidents and improvements A.14.1 Information security aspects of business continuity management	4.2.2(b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities 5.1(c) establishing roles and responsibilities for information security A.8.1.1 Roles and responsibilities A.13.2.1 Responsibilities and procedures A.14.1 Information security aspects of business continuity management (all)	Roles and responsibilities mentioned but not specific to CSPs or relevant parties. Consider incident response as part of business continuity.
11.1.2(b)	INCREMENTAL	A.13.1 Reporting information security events and weaknesses A.6.1 Internal organization	A.13.1.1 Reporting information security events A.6.1.2 Information security coordination A.6.1.6 Contact with authorities A.6.1.7 Contact with special interest groups	Implementation of contact procedures was not explicitly mentioned.
11.1.2(c)	NEW	N.A	N.A	Definition of the extent of cooperation in the Service Level Agreement (SLA) was not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11.1.2(d)	INCLUDED	4.2.3 Monitor and review the ISMS 8.3 Preventive action A.13.2 Management of information security incidents and improvements	4.2.3(a5) determine whether the actions taken to resolve a breach of security were effective 4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS 8.3 Preventive action (all) A.13.2.2 Learning from information security incidents	N.A
11.1.2(e)	INCREMENTAL	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvements A.14.1 Information security aspects of business continuity management	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a)) 4.2.3(a) Execute monitoring and reviewing procedures and other controls A.13.1.1 Reporting information security events A.13.2.1 Responsibilities and procedures A.14.1 Information security aspects of business continuity management (all)	Incident response in general mentioned but not the escalation, recovery and resolution procedures/time frames. Consider incident response as part of business continuity.
11.1.2(f)	INCLUDED	A.13.2 Management of information security incidents and improvements	A.13.2.2 Learning from information security incidents	N.A
11.1.2(g)	INCREMENTAL	A.13.2 Management of information security incidents and improvements	A.13.2.2 Learning from information security incidents	Quantification and monitoring mentioned but not classification by severity levels and priorities.
11.1.2(h)	INCREMENTAL	A.6.2 External parties A.10.8 Exchange of information	A.6.2.2 Addressing security when dealing with customers A.10.8.1 Information exchange policies and procedures A.10.8.2 Exchange agreements A.10.8.3 Physical media in transit	Notification to customers about any security breach is not mentioned.
11.1.2(i)	INCREMENTAL	A.13.2 Management of information security incidents and improvements	A.13.2.3 Collection of evidence	Collection of evidence mentioned but not the capability to provide consumers with evidence.
11.1.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11.1.3(a)	INCREMENTAL	5.1 Management commitment 5.2.1 Provision of resources A.6.1 Internal organization A.14.1 Information security aspects of business continuity management	5.1(c) establishing roles and responsibilities for information security 5.1(e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1) 5.2.1(a) establish, implement, operate, monitor, review, maintain and improve an ISMS A.6.1.3 Allocation of information security responsibilities A.14.1 Information security aspects of business continuity management (all)	Roles and responsibilities and resources mentioned but not specifically about having designated personnel available to respond to events. Consider incident response as part of business continuity.
11.1.3(b)	INCLUDED	A.15.1 Compliance with legal requirements	A.15.1.1 Identification of applicable legislation	N.A
11.1.3(c)	INCLUDED	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS A.13.2 Management of information security incidents and improvements	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3a) 4.2.3(a) Execute monitoring and reviewing procedures and other controls A.13.2.1 Responsibilities and procedures	N.A
11.1.3(d)	INCREMENTAL	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS A.13.2 Management of information security incidents and improvements A.14.1 Information security aspects of business continuity management	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3a) 4.2.3(a) Execute monitoring and reviewing procedures and other controls A.13.2.1 Responsibilities and procedures A.14.1 Information security aspects of business continuity management (all)	Incident response in general mentioned but not procedures for escalation. Consider incident response as part of business continuity.
11.1.3(e)	INCREMENTAL	A.6.2 External parties A.10.8 Exchange of information A.13.1 Reporting information security events and weaknesses	A.6.2.2 Addressing security when dealing with customers A.10.8.1 Information exchange policies and procedures A.10.8.2 Exchange agreements A.13.1.1 Reporting information security events	Notification to customers on the impact is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11.1.4 Level 3 requirements				
11.1.4(a)	INCREMENTAL	A.10.6 Network security management A.13.2 Management of information security incidents and improvements	A.10.6 Network security management (all) A.13.2.1 Responsibilities and procedures	Security measures and network controls are mentioned in general, but not tools, specific network equipment or source code review.
11.1.4(b)	NEW	A.13.1 Reporting information security events and weaknesses	A.13.1.1 Reporting information security events	N.A
11.1.4(c)	NEW	A.13.1 Reporting information security events and weaknesses	A.13.1.1 Reporting information security events	Notification to customers about major security incidents is not mentioned.
11.1.4(d)	INCLUDED	4.2.2 Implement and operate the ISMS A.13.2 Management of information security incidents and improvements	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a)) A.13.2.3 Collection of evidence	N.A
11.2 Information security incident response plan testing and updates				
11.2.1 General				
Control Objective	NEW	5.0 Management responsibility A.8 Human resources security A.13 Information security incident management A.14 Business continuity management	N.A	N.A
11.2.2 Level 1 requirements				
11.2.2(a)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1 Information security aspects of business continuity management (all)	No mention of test plan for incident response plan. Consider incident response as part of business continuity.
11.2.2(b)	NEW	N.A	N.A	No mention of the frequency of testing for the incident response plan.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11.2.2(c)	INCREMENTAL	5.2.2 Training, awareness and competence A.8.2 During employment A.13.2 Management of information security incidents and improvements A.14.1 Information security aspects of business continuity management	5.2.2 Training, awareness and competence (all) A.8.2.2 Information security awareness, education and training A.13.2.1 Responsibilities and procedures A.14.1 Information security aspects of business continuity management (all)	Security training in general and not specific to incident response responsibilities. Consider incident response as part of business continuity.
11.2.3 Level 2 requirements				
11.2.3(a)	INCREMENTAL	A.13.2 Management of information security incidents and improvements A.14.1 Information security aspects of business continuity management	A.13.2.1 Responsibilities and procedures A.14.1 Information security aspects of business continuity management (all)	No mention of requirement to maintain plan up to date in accordance with the industry standards. Consider incident response as part of business continuity.
11.2.4 Level 3 requirements				
11.2.4(a)	NEW	N.A	N.A	No mention of drills and the frequency.
11.3 Information security incident reporting				
11.3.1 General				
Control Objective	INCLUDED	A.13 Information security incident management	N.A	N.A
11.3.2 Level 1 requirements				
11.3.2(a)	INCLUDED	A.13.1 Reporting information security events and weaknesses	A.13.1.1 Reporting information security events	N.A
11.3.2(b)	INCREMENTAL	A.13.1 Reporting information security events and weaknesses	A.13.1.1 Reporting information security events	While reporting of information security events through appropriate management channels is mentioned, notification specific to customers and affected third parties about the security breach is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
11.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
11.4 Problem management				
11.4.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility A.8 Human resources security A.13 Information security incident management	N.A	Requirements on incident management reporting are mentioned generally.
11.4.2 Level 1 requirements				
11.4.2(a)	INCLUDED	4.2.1 Establish the ISMS 8.2 Corrective action 8.3 Preventive action	4.2.1(d) Identify the risks 4.2.1(e) Analyze and evaluate the risks 4.2.1(f) Identify and evaluate options for the treatment of risks 8.2 Corrective action (all) 8.3 Preventive action (all)	N.A
11.4.2(b)	INCLUDED	4.2.2 Implement and operate the ISMS 5.1 Management commitment A.8.1 Prior to employment A.13.2 Management of information security incidents and improvements	4.2.2(b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities 5.1(c) establishing roles and responsibilities for information security A.8.1.1 Roles and responsibilities A.13.2.1 Responsibilities and procedures	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
11.4.2(c)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS	4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.2(a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5) 4.2.2(b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities	Establishment of escalation process for problems with different severity levels not explicitly mentioned though risk treatment plans could include an escalation process/procedure.
11.4.3 Level 2 requirements				
11.4.3(a)	INCREMENTAL	4.2 Establishing and managing the ISMS 8.1 Continual improvement 8.2 Corrective action 8.3 Preventive action	4.2.4(b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learned from the security experiences of other organizations and those of the organization itself 8.1 Continual improvement 8.2(e) recording results of action taken (see 4.3.3) 8.3(d) recording results of action taken (see 4.3.3)	Trend analysis was not explicitly mentioned but analysis of events and recording of results could imply a development of a similar tool.
11.4.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12 Data Governance				
12.1 Data classification				
12.1.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.7 Asset management A.11 Access control	N.A	N.A
12.1.2 Level 1 requirements **No applicable Level 1 controls.**				
12.1.3 Level 2 requirements				
12.1.3(a)	INCLUDED	4.2.1 Establish the ISMS 4.3.2 Control of documents A.7.2 Information classification A.11.6 Application and information access control	4.2.1(g) Select control objectives and controls for the treatment of risks 4.3.2(f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification A.7.2.2 Information labeling and handling A.11.6.2 Sensitive system isolation	N.A
12.1.3(b)	INCLUDED	A.7.2 Information classification A.10.7 Media handling	A.7.2.1 Classification guidelines A.10.7.3 Information handling procedures	N.A
12.1.3(c)	INCREMENTAL	A.7.2 Information classification A.10.7 Media handling	A.7.2.1 Classification guidelines A.10.7.3 Information handling procedures	Classification guidelines mentioned are for information but could possibly be applied to assets, including communication channels.
12.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.2 Data ownership				
12.2.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	4.0 ISMS A.6 Organization of information security A.7 Asset management A.8 Human resources security	N.A	N.A
12.2.2 Level 1 requirements **No applicable Level 1 controls.**				
12.2.3 Level 2 requirements				
12.2.3(a)	INCLUDED	4.2.1 Establish the ISMS A.6.1 Internal organization A.6.2 External parties A.7.1 Responsibility for assets A.8.1 Prior to employment	4.2.1(d1) Identify the assets within the scope of the ISMS, and the owners of these assets A.6.1.3 Allocation of information security responsibilities A.6.2.3 Addressing security in third party agreements A.7.1.1 Inventory of assets A.7.1.2 Ownership of assets A.8.1.1 Roles and responsibilities A.8.1.3 Terms and conditions of employment	N.A
12.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.3 Data integrity				
12.3.1 General				
Control Objective	INCLUDED	A.12 Information systems acquisition, development and maintenance	N.A	N.A
12.3.2 Level 1 requirements **No applicable Level 1 controls.**				
12.3.3 Level 2 requirements				
12.3.3(a)	INCLUDED	A.12.2 Correct processing in applications	A.12.2 Correct processing in applications (all)	N.A
12.3.3(b)	INCREMENTAL	A.12.2 Correct processing in applications	A.12.2 Correct processing in applications (all)	Authenticity not mentioned explicitly but could be covered under ISO/IEC 27001:2005 Section A.12.2.2 Control of internal processing.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.4 Data labeling / handling				
12.4.1 General				
Control Objective	INCREMENTAL	A.7 Asset management A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
12.4.2 Level 1 requirements				
12.4.2(a)	INCLUDED	A.7.2 Information classification	A.7.2.2 Information labeling and handling	N.A
12.4.3 Level 2 requirements				
12.4.3(a)	INCREMENTAL	A.7.1 Responsibility for assets A.10.7 Media handling	A.7.1.1 Inventory of assets A.10.7.3 Information handling procedures	Maintenance logs are not mentioned explicitly though maintenance itself is.
12.4.3(b)	INCLUDED	A.10.7 Media handling A.10.8 Exchange of information A.10.9 Electronic commerce services A.12.2 Correct processing in applications A.12.3 Cryptographic controls	A.10.7.3 Information handling procedures A.10.8.1 Information exchange policies and procedures A.10.8.2 Exchange agreements A.10.8.4 Electronic messaging A.10.8.5 Business information systems A.10.9 Electronic commerce services (all) A.12.2 Correct processing in applications (all) A.12.3.1 Policy on the use of cryptographic controls	N.A
12.4.3(c)	NEW	N.A	N.A	Requirement on location of data storage is not mentioned.
12.4.4 Level 3 requirements				
12.4.4(a)	NEW	N.A	N.A	Requirement on maintenance of logs and inventories of physical locations of cloud user data is not mentioned.
12.4.4(b)	INCREMENTAL	A.10.7 Media handling	A.10.7.2 Disposal of media	Documentation of such procedures is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.5 Data protection				
12.5.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance A.15 Compliance	N.A	N.A
12.5.2 Level 1 requirements				
12.5.2(a)	INCREMENTAL	A.10.7 Media handling	A.10.7.3 Information handling procedures	Media is mentioned in general. However, specific media, virtualised images and snapshots are not mentioned.
12.5.2(b)	INCLUDED	A.10.8 Exchange of information	A.10.8.3 Physical media in transit	N.A
12.5.3 Level 2 requirements				
12.5.3(a)	INCREMENTAL	A.10.7 Media handling	A.10.7.3 Information handling procedures	Storage of information is mentioned but not the review of the security of the storage.
12.5.3(b)	INCREMENTAL	A.7.2 Information classification A.9.1 Secure areas A.9.2 Equipment security A.12.2 Correct processing in applications A.12.5 Security in development and support processes	A.7.2.2 Information labeling and handling A.9.1.1 Physical security perimeter A.9.1.2 Physical entry controls A.9.1.5 Working in secure areas A.9.2.4 Equipment maintenance A.9.2.5 Security of equipment off premises A.12.2 Correct processing in applications (all) A.12.5.4 Information leakage	Logical access security to data and physical access security to backup media are not mentioned.
12.5.3(c)	INCREMENTAL	A.12.3 Cryptographic control	A.12.3.1 Policy on the use of cryptographic controls	Cryptography usage in general is mentioned but not specifically requiring having strong encryption for end point devices.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.5.3(d)	INCREMENTAL	4.2.2 Implement and operate the ISMS	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a))	Virtualised images-specific security controls are not mentioned.
12.5.4 Level 3 requirements				
12.5.4(a)	INCREMENTAL	A.9.2 Equipment securityA.12.2 Correct processing in applicationsA.12.5 Security in development and support processesA.15.1 Compliance with legal requirements	A.9.2.1 Equipment siting and protection A.9.2.2 Supporting utilities A.9.2.3 Cabling security A.9.2.4 Equipment maintenance A.9.2.5 Security of equipment off premises A.9.2.7 Removal of property A.12.2 Correct processing in applications (all) A.12.5.4 Information leakage A.15.1.4 Data protection and privacy of personal information	Data validation/protection and equipment security in general mentioned no explicit mention of data loss prevention strategy.
12.6 Data retention				
12.6.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security A.10 Communications and operations management A.13 Information security incident management	N.A	N.A
12.6.2 Level 1 requirements **No applicable Level 1 controls.**				
12.6.3 Level 2 requirements				
12.6.3(a)	INCREMENTAL	A.10.5 Back-up A.10.7 Media handling	A.10.5.1 Information back-up A.10.7.3 Information handling procedures	Backup policy is mentioned in general but not the implementation of backup or redundancy mechanisms.
12.6.3(b)	INCLUDED	A.10.5 Back-up	A.10.5.1 Information back-up	N.A
12.6.3(c)	INCLUDED	A.9.2 Equipment security A.10.7 Media handling	A.9.2.6 Secure disposal or re-use of equipment A.10.7.2 Disposal of media	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.6.3(d)	INCREMENTAL	4.3.3 Control of records	4.3.3 Control of records	Brief mention of retention controls to be in place but no specific mechanism and retention rules stated.
12.6.3(e)	INCLUDED	A.10.10 Monitoring A.13.2 Management of information security incidents and improvements	A.10.10.1 Audit logging A.10.10.3 Protection of log information A.13.2.3 Collection of evidence	N.A
12.6.4 Level 3 requirements				
12.6.4(a)	NEW	N.A	N.A	Provision of mechanisms for cloud users to remove/destroy all data is not mentioned.
12.6.4(b)	INCLUDED	4.3.3 Control of records	4.3.3 Control of records	N.A
12.7 Data backups				
12.7.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security A.10 Communications and operations management	N.A	N.A
12.7.2 Level 1 requirements				
12.7.2(a)	INCLUDED	A.10.5 Back-up A.10.8 Exchange of information	A.10.5.1 Information back-up A.10.8.3 Physical media in transit	N.A
12.7.2(b)	INCREMENTAL	A.10.5 Back-up	A.10.5.1 Information back-up	Backups are mentioned in general but not the frequency of the testing of backups.
12.7.2(c)	INCREMENTAL	A.9.2 Equipment security A.10.5 Back-up	A.9.2.5 Security of equipment off premises A.10.5.1 Information back-up	Backups and security of equipment off premises mentioned in general but not procedures to determine access and storage locations of backups.
12.7.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
12.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.8 Secure disposal and decommissioning of hardcopy, media and equipment				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.8.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security A.10 Communications and operations management	N.A	N.A
12.8.2 Level 1 requirements				
12.8.2(a)	INCLUDED	A.9.2 Equipment security A.10.7 Media handling	A.9.2.6 Secure disposal or re-use of equipment A.10.7.2 Disposal of media	N.A
12.8.2(b)	INCLUDED	A.9.2 Equipment security	A.9.2.6 Secure disposal or re-use of equipment	To securely overwrite storage media would imply having storage media be forensically erased.
12.8.2(c)	NEW	N.A	N.A	Specific procedures to securely dispose hardcopy materials containing data are not mentioned.
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 verification of live instances and backups				
12.9.1 General				
Control Objective	INCREMENTAL	N.A	N.A	N.A
12.9.2 Level 1 requirements **No applicable Level 1 controls.**				
12.9.3 Level 2 requirements				
12.9.3(a)	INCREMENTAL	A.9.2 Equipment security A.10.7 Media handling	A.9.2.6 Secure disposal or re-use of equipment A.10.7.2 Disposal of media	Procedure to verify that data has been securely removed is not mentioned.
12.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.10 Tracking of data				
12.10.1 General				
Control Objective	NEW	N.A	N.A	Provision of mechanisms for cloud users to track data is not mentioned.
12.10.2 Level 1 requirements **No applicable Level 1 controls.**				
12.10.3 Level 2 requirements				
12.10.3(a)	NEW	N.A	N.A	Making available location information of data in production/backup environments is not mentioned.
12.10.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
12.11 Production data				
12.11.1 General				
Control Objective	NEW	4.0 ISMS 5.0 Management responsibility A.5 Security policy A.10 Communications and operations management	N.A	N.A
12.11.2 Level 1 requirements **No applicable Level 1 controls.**				
12.11.3 Level 2 requirements				
12.11.3(a)	INCREMENTAL	A.10.1 Operational procedures and responsibilities	A.10.1.4 Separation of development, test and operational facilities	Segregation of environments is mentioned but controls to prohibit extraction/transfer of production data to non-production media is not.
12.11.3(b)	INCREMENTAL	A.10.9 Electronic commerce services	A.10.9.2 On-line transactions	Brief mention of data duplication in a smaller context.
12.11.3(c)	INCREMENTAL	A.10.1 Operational procedures and responsibilities	A.10.1.4 Separation of development, test and operational facilities	Segregation of environments is mentioned but procedures for sanitization/approval before using production data in non-production environment are not.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
12.11.3(d)	INCREMENTAL	4.2.1 Establish the ISMS 4.3.1 General 5.1 Management commitment A.5.1 Information security policy	4.2.1(b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology 4.3.1(a) documented statements of the ISMS policy and objectives 5.1(d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement A.5.1.1 Information security policy document	Establishment and communication of information security policy is mentioned. However, specific topic about copying production data into non-production environments is not mentioned.
12.11.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
13 Audit logging and monitoring				
13.1 Logging and monitoring process				
13.1.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.10 Communications and operations management	N.A	N.A
13.1.2 Level 1 requirements				
13.1.2(a)	INCLUDED	A.10.10 Monitoring	A.10.10.4 Administrator and operator logs	N.A
13.1.2(b)	INCLUDED	A.10.10 Monitoring	A.10.10.5 Fault logging	N.A
13.1.2(c)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use	N.A
13.1.2(d)	INCLUDED	A.10.10 Monitoring	A.10.10.3 Protection of log information	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
13.1.2(e)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use	N.A
13.1.2(f)	INCREMENTAL	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use	Audit logging and log review mentioned in general, not specific to logging and review of identification / authentication mechanism usage.
13.1.2(g)	INCLUDED	A.10.10 Monitoring	A.10.10.6 Clock synchronization	N.A
13.1.2(h)	INCLUDED	A.10.10 Monitoring	A.10.10.2 Monitoring system use	N.A
13.1.3 Level 2 requirements				
13.1.3(a)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging	N.A
13.1.3(b)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging	N.A
13.1.3(c)	INCLUDED	A.10.10 Monitoring	A.10.10.4 Administrator and operator logs	N.A
13.1.3(d)	INCREMENTAL	A.10.10 Monitoring	A.10.10.3 Protection of log information	Protection of logs in general, implementation of integrity monitoring or change detection software not mentioned.
13.1.3(e)	NEW	N.A	N.A	Intrusion Detection and Prevention Systems (IDPS) is not a requirement of ISO/IEC 27001:2005.
13.1.4 Level 3 requirements				
13.1.4(a)	INCLUDED	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a)) 4.2.3(a) Execute monitoring and reviewing procedures and other controls	N.A
13.1.4(b)	INCLUDED	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a)) 4.2.3(a) Execute monitoring and reviewing procedures and other controls	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
13.1.4(c)	INCLUDED	4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a)) 4.2.3(a) Execute monitoring and reviewing procedures and other controls	N.A
13.1.4(d)	NEW	N.A	N.A	Following up, verification and addressing of alerts are not mentioned.
13.2 Log review				
13.2.1 General				
Control Objective	NEW	A.10 Communications and operations management	N.A	N.A
13.2.2 Level 1 requirements				
13.2.2(a)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use	N.A
13.2.3 Level 2 requirements				
13.2.3(a)	INCREMENTAL	A.10.10 Monitoring	A.10.10.1 Audit logging A.10.10.2 Monitoring system use	Periodical review is mentioned but not a specific frequency.
13.2.4 Level 3 requirements				
13.2.4(a)	NEW	N.A	N.A	Requirement of having an automated tool for monitoring of logs is not mentioned.
13.3 Audit trails				
13.3.1 General				
Control Objective	INCLUDED	A.10 Communications and operations management	N.A	N.A
13.3.2 Level 1 requirements				
13.3.2(a)	INCREMENTAL	A.10.10 Monitoring	A.10.10.1 Audit logging	Audit trail mentioned in general, but specific details captured are not mentioned.
13.3.2(b)	INCLUDED	A.10.10 Monitoring	A.10.10.3 Protection of log information	N.A
12.3.3 Level 2 requirements				
12.3.3(a)	INCREMENTAL	A.10.10 Monitoring	A.10.10.3 Protection of log information	Media to be used for capturing audit trails is not explicitly mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
13.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
13.4 Backup and retention of audit trails				
13.4.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management	N.A	N.A
13.4.2 Level 1 requirements				
13.4.2(a)	INCLUDED	A.10.10 Monitoring	A.10.10.1 Audit logging	N.A
13.4.3 Level 2 requirements				
13.4.3(a)	INCREMENTAL	A.10.10 Monitoring	A.10.10.3 Protection of log information	Backing up of logs is not mentioned.
13.4.3(b)	INCLUDED	A.10.10 Monitoring A.11.2 User access management A.11.4 Network access control	A.10.10.3 Protection of log information A.11.2.2 Privilege management A.11.4.5 Segregation in networks A.11.4.6 Network connection control A.11.4.7 Network routing control	N.A
13.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
13.5 Usage logs				
13.5.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management	N.A	N.A
13.5.2 Level 1 requirements				
13.5.2(a)	INCREMENTAL	A.10.10 Monitoring	A.10.10.3 Protection of log information	Protection of logs in general is mentioned but not specifically having strict files and directories' permissions.
13.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
13.5.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
14 Secure configuration				
14.1 Server and network device configuration standards				
14.1.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management	N.A	No mention of industry accepted system hardening standards.
14.1.2 Level 1 requirements				
14.1.2(a)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	Network security management and controls implementation in general although details are not mentioned.
14.1.2(b)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	
14.1.2(c)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	
14.1.2(d)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	
14.1.2(e)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	
14.1.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.1.4 Level 3 requirements				
14.1.4(a)	NEW	N.A	N.A	No mention of compliance to Common Criteria EAL4 or similar.
14.2 Malicious code prevention				
14.2.1 General				
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility A.8 Human resources security A.10 Communications and operations management	N.A	N.A
14.2.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
14.2.2(a)	INCLUDED	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	N.A
14.2.2(b)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	Controls against malicious codes are mentioned but specific requirements are not mentioned.
14.2.2(c)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	
14.2.2(d)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	
14.2.2(e)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	
14.2.2(f)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	
14.2.2(g)	INCREMENTAL	4.2.2 Implement and operate the ISMS 5.2.2 Training, awareness and competence A.8.2 During employment	4.2.2(e) Implement training and awareness programs (see 5.2.2) 5.2.2 Training, awareness and competence (all) A.8.2.2 Information security awareness, education and training	Awareness in general is mentioned, specific topics for administrations of cloud systems not mentioned.
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(a)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	Controls against malicious codes are mentioned but periodic testing is not mentioned.
14.2.4(b)	INCREMENTAL	A.10.4 Protection against malicious and mobile code	A.10.4.1 Controls against malicious code	Controls against malicious codes are mentioned but specific control requirements are not mentioned.
14.3 Portable code				
14.3.1 General				
Control Objective	INCLUDED	A.10 Communications and operations management	N.A	N.A
14.3.2 Level 1 requirements				
14.3.2(a)	INCLUDED	A.10.4 Protection against malicious and mobile code	A.10.4.2 Controls against mobile code	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
14.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.4 Physical port protection				
14.4.1 General				
Control Objective	INCREMENTAL	A.11 Access control	N.A	N.A
14.4.2 Level 1 requirements				
14.4.2(a)	INCLUDED	A.11.4 Network access control	A.11.4.4 Remote diagnostic and configuration port protection	"Physical and logical access to diagnostic and configuration ports shall be controlled" covers the requirement.
14.4.2(b)	INCREMENTAL	A.11.4 Network access control	A.11.4.4 Remote diagnostic and configuration port protection	"Physical and logical access to diagnostic and configuration ports shall be controlled" partially covers the requirement.
14.4.2(c)	INCREMENTAL	A.11.4 Network access control	A.11.4.4 Remote diagnostic and configuration port protection	"Physical and logical access to diagnostic and configuration ports shall be controlled" partially covers the requirement.
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 Restrictions to system utilities				
14.5.1 General				
Control Objective	INCLUDED	A.11 Access control	N.A	N.A
14.5.2 Level 1 requirements				
14.5.2(a)	INCLUDED	A.11.5 Operating system access control	A.11.5.4 Use of system utilities	N.A
14.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
14.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.6 System and network session management				
14.6.1 General				
Control Objective	INCLUDED	A.11 Access control	N.A	N.A
14.6.2 Level 1 requirements				
14.6.2(a)	INCLUDED	A.11.5 Operating system access control	A.11.5.5 Session time-out	N.A
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 Unnecessary service and protocols				
14.7.1 General				
Control Objective	INCREMENTAL	A.10.6 Network security management	N.A	N.A
14.7.2 Level 1 requirements				
14.7.2(a)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	Network security mentioned in general although details are not mentioned.
14.7.2(b)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	Network security mentioned in general although details are not mentioned.
14.7.2(c)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	Network security mentioned in general although details are not mentioned.
14.7.3 Level 2 requirements				
14.7.3(a)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	Network security in general although details are not mentioned.
14.7.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.8 Unauthorised software				
14.8.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	A.12 Information systems acquisition, development and maintenance	N.A	N.A
14.8.2 Level 1 requirements				
14.8.2(a)	INCLUDED	A.12.4 Security of system files A.12.5 Security in development and support processes	A.12.4.1 Control of operational software A.12.5.3 Restrictions on changes to software packages	Procedures in place would imply having mechanisms in place.
14.8.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
14.8.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
14.9 Enforcement checks				
14.9.1 General				
Control Objective	INCREMENTAL	A.15 Compliance	N.A	N.A
14.9.2 Level 1 requirements				
14.9.2(a)	INCLUDED	A.15.2 Compliance with security policies and standards, and technical compliance	A.15.2.2 Technical compliance checking	N.A
14.9.3 Level 2 requirements				
14.9.3(a)	INCREMENTAL	A.15.2 Compliance with security policies and standards, and technical compliance	A.15.2.2 Technical compliance checking	Frequency of compliance checks is not mentioned.
14.9.3(b)	NEW	N.A	N.A	Implementation of file integrity monitoring tools is not mentioned.
14.9.4 Level 3 requirements				
14.9.4(a)	INCREMENTAL	A.15.2 Compliance with security policies and standards, and technical compliance	A.15.2.2 Technical compliance checking	Frequency of compliance checks is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
14.9.4(b)	NEW	N.A	N.A	Implementation of file integrity monitoring tools is not mentioned.

9.10 Security testing and monitoring

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
15 Security testing and monitoring				
15.1 Vulnerability scanning				
15.1.1 General				
Control Objective	NEW	4.0 ISMS	N.A	N.A
15.1.2 Level 1 requirements				
15.1.2(a)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(d3) Identify the vulnerabilities that might be exploited by the threats	Identification of vulnerabilities is mentioned, but specific usage of vulnerability scanning is not. Frequency of such scans is also not mentioned.
15.1.2(b)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS	4.2.1(e2) Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented 4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.2(c) Implement controls selected in 4.2.1(g) to meet the control objectives	Evaluation of vulnerabilities and implementation of controls to address vulnerabilities are mentioned in general. Usage of Common Vulnerability Scoring System (CVSS) scoring and the addressing vulnerabilities within one week are not mentioned.
15.1.3 Level 2 requirements				
15.1.3(a)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(d3) Identify the vulnerabilities that might be exploited by the threats	Identification of vulnerabilities is mentioned, but specific usage of vulnerability scanning is not. Frequency of such scans is also not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
15.1.3(b)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS	4.2.1(e2) Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented 4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.2(c) Implement controls selected in 4.2.1g) to meet the control objectives	Evaluation of vulnerabilities and implementation of controls to address vulnerabilities are mentioned in general. Usage of Common Vulnerability Scoring System (CVSS) scoring and the addressing vulnerabilities within one week are not mentioned.
15.1.4 Level 3 requirements				
15.1.4(a)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(d3) Identify the vulnerabilities that might be exploited by the threats	Identification of vulnerabilities is mentioned, but specific usage of vulnerability scanning is not. Frequency of such scans is also not mentioned.
15.2 Penetration testing				
15.2.1 General				
Control Objective	NEW	N.A	N.A	Penetration testing is not mentioned in ISO/IEC 27001:2005.
15.2.2 Level 1 requirements				
15.2.2(a)	NEW	N.A	N.A	Penetration testing is not mentioned in ISO/IEC 27001:2005.
15.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
15.2.4 Level 3 requirements				
15.2.4(a)	NEW	N.A	N.A	Penetration testing is not mentioned in ISO/IEC 27001:2005.
15.3 Security monitoring				
15.3.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	4.0 ISMS 5.0 Management responsibility 7.0 Management review of the ISMS A.5 Security policy A.12 Information systems acquisition, development and maintenance	N.A	N.A
15.3.2 Level 1 requirements				
15.3.2(a)	INCLUDED	4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS A.12.6 Technical Vulnerability Management	4.2.1(d3) Identify the vulnerabilities that might be exploited by the threats 4.2.1(e) Analyze and evaluate the risks. 4.2.1(f) Identify and evaluate options for the treatment of risks 4.2.1(g) Select control objectives and controls for the treatment of risks 4.2.2(c) Implement controls selected in 4.2.1(g) to meet the control objectives A.12.6.1 Control of technical vulnerabilities	N.A
15.3.2(b)	NEW	N.A	N.A	Implementation of intrusion detection systems and/or intrusion prevention systems not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
15.3.2(c)	INCREMENTAL	4.2.1 Establish the ISMS 4.2.3 Monitor and review the ISMS 4.3.1 General 5.1 Management commitment 7.1 General A.5.1 Information security policy	4.2.1(b1) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security 4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties 4.3.1(a) documented statements of the ISMS policy and objectives 5.1(a) establishing an ISMS policy 7.1 General A.5.1.2 Review of the information security policy	Specific topics about network intrusion, detection and prevention are not mentioned.
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(a)	INCREMENTAL	5.2.2 Training, awareness and competence A.15.2 Compliance with security policies and standards, and technical compliance	5.2.2(a) determining the necessary competencies for personnel performing work effecting the ISMS 5.2.2(d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3) A.15.2.2 Technical compliance checking	Identification and establishment of depth and scope of compliance review not mentioned. Assessing technical competencies not explicitly mentioned though ISO/IEC 27001:2005 Section 5.2.2 could lead to the technical assessment of the personnel.

9.11 System acquisitions and development

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
16 System acquisitions and development				
16.1 Development, acquisition and release management				
16.1.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management A.11 Access control A.12 Information systems acquisition, development and maintenance	N.A	N.A
16.1.2 Level 1 requirements				
16.1.2(a)	INCREMENTAL	A.12.1 Security requirements of information systems A.12.5 Security in development and support processes	A.12.1.1 Security requirements analysis and specification A.12.5.5 Outsourced software development	Development of applications in accordance with industry accepted practices is not mentioned though security principles are included during the system development life cycle (SDLC) phase under ISO/IEC 27001:2005 Section A.12.1.1.
16.1.2(b)	INCREMENTAL	A.6.2 External parties	A.6.2.2 Addressing security when dealing with customers	Addressing security requirements before giving access to customers mentioned but not the specific actions (e.g., removal of custom accounts, IDs and passwords).
16.1.2(c)	INCREMENTAL	A.6.2 External parties A.10.1 Operational procedures and responsibilities A.12.4 Security of system files	A.6.2.2 Addressing security when dealing with customers A.10.1.4 Separation of development, test and operational facilities A.12.4.2 Protection of system test data	Removal of test data and accounts is not mentioned.
16.1.2(d)	INCREMENTAL	A.12.1 Security requirements of information systems	A.12.1.1 Security requirements analysis and specification	Security principles are included during the system development life cycle (SDLC) phase under ISO/IEC 27001:2005 Section A.12.1.1 but verification against industry standards is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
16.1.2(e)	INCLUDED	A.10.1 Operational procedures and responsibilities A.11.4 Network access control	A.10.1.4 Separation of development, test and operational facilities A.11.4.5 Segregation in networks	N.A
16.1.2(f)	INCLUDED	A.12.5 Security in development and support processes	A.12.5.3 Restrictions on changes to software packages	N.A
16.1.2(g)	INCLUDED	A.10.3 System planning and acceptance A.12.4 Security of system files	A.10.3.2 System acceptance A.12.4.2 Protection of system test data	N.A
16.1.2(h)	INCLUDED	A.12.1 Security requirements of information systems	A.12.1.1 Security requirements analysis and specification	N.A
16.1.2(i)	INCLUDED	A.12.2 Correct processing in applications	A.12.2.1 Input data validation	N.A
16.1.2(j)	NEW	N.A	N.A	N.A
16.1.2(k)	NEW	N.A	N.A	N.A
16.1.2(l)	NEW	N.A	N.A	N.A
16.1.3 Level 2 requirements				
16.1.3(a)	NEW	N.A	N.A	N.A
16.1.4 Level 3 requirements				
16.1.4(a)	NEW	N.A	N.A	N.A
16.2 Web application security				
16.2.1 General				
Control Objective	NEW	A.12 Information systems acquisition, development and maintenance	N.A	N.A
16.2.2 Level 1 requirements **No applicable Level 1 controls.**				
16.2.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
16.2.3(a)	INCREMENTAL	A.12.5 Security in development and support processes	A.12.5.1 Change control procedures	Change control procedures are mentioned in general but not specifically the reviewing of web applications using assessment tools periodically. Minimum requirement is also not mentioned.
16.2.3(b)	INCLUDED	A.10.6 Network security management	A.10.6 Network security management (all)	N.A
16.2.3(c)	NEW	N.A	N.A	N.A
16.2.4 Level 3 requirements				
16.2.4(a)	NEW	N.A	N.A	N.A
16.3 System testing				
16.3.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
16.3.2 Level 1 requirements				
16.3.2(a)	INCLUDED	A.12.4 Security of system files	A.12.4.2 Protection of system test data	N.A
16.3.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
16.3.3(a)	INCREMENTAL	A.6.2 External parties A.10.3 System planning and acceptance A.12.1 Security requirements of information systems A.12.4 Security of system files A.12.5 Security in development and support processes	A.6.2.2 Addressing security when dealing with customers A.10.3.2 System acceptance A.12.1.1 Security requirements analysis and specification A.12.4.2 Protection of system test data A.12.5.5 Outsourced software development	While some elements of a systematic monitoring and evaluation program exist, most are not mentioned (e.g., management oversight, source code review, usage of production data for test/development purposes).
16.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
16.4 Source code security				
16.4.1 General				
Control Objective	INCLUDED	A.12 Information systems acquisition, development and maintenance	N.A	N.A
16.4.2 Level 1 requirements				
16.4.2(a)	INCREMENTAL	A.12.4 Security of system files	A.12.4.3 Access control to program source code	Enforcement of version control is not mentioned.
16.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
16.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
16.5 Outsourced software development				
16.5.1 General				
Control Objective	INCLUDED	A.12 Information systems acquisition, development and maintenance	N.A	N.A
16.5.2 Level 1 requirements				
16.5.2(a)	INCLUDED	A.12.5 Security in development and support processes	A.12.5.5 Outsourced software development	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
16.5.3 Level 2 requirements				
16.5.3(a)	INCREMENTAL	A.12.5 Security in development and support processes	A.12.5.5 Outsourced software development	While supervision and monitoring of outsourced development is mentioned, specific objective to ensure performance in accordance with industry standards and regulatory requirements is not.
16.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

9.12 Encryption

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
17 Encryption				
17.1 Encryption policies and procedures				
17.1.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
17.1.2 Level 1 requirements				
17.1.2(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3 Cryptographic controls (all)	Usage of cryptography controls mentioned in general but specific topics are not.
17.1.2(b)	INCREMENTAL	A.10.6 Network security management A.10.8 Exchange of information A.10.9 Electronic commerce services	A.10.6.1 Network controls A.10.8.1 Information exchange policies and procedures A.10.8.4 Electronic messaging A.10.8.5 Business information systems A.10.9.1 Electronic commerce A.10.9.2 On-line transactions	While protection of information is mentioned, the specific usage of encryption is not.
17.1.3 Level 2 requirements **The requirements are the same as those in Level 1.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
17.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
17.2 Channel encryption				
17.2.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
17.2.2 Level 1 requirements				
17.2.2(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls	Usage of cryptography in general is mentioned but not specifically for non-console administrative access.
17.2.2(b)	INCLUDED	A.10.9 Electronic commerce services A.12.3 Cryptographic controls	A.10.9.1 Electronic commerce A.10.9.2 On-line transactions A.12.3.1 Policy on the use of cryptographic controls	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 Key management				
17.3.1 General				
17.3.1	INCREMENTAL	A.12 Information systems acquisition, development and maintenance	N.A	N.A
17.3.2 Level 1 requirements				
17.3.2(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls	Policy on use of cryptography mentioned in general.
17.3.2(b)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls	Policy on use of cryptography mentioned in general.
17.3.2(c)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	Key changing procedures are not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
17.3.2(d)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	Formal acknowledgement of responsibilities is not mentioned.
17.3.3 Level 2 requirements				
17.3.3(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	Specific requirement is not mentioned.
17.3.3(b)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	
17.3.3(c)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	
17.3.3(d)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	
17.3.3(e)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	
17.3.3(f)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3 Cryptographic controls (all)	
17.3.3(g)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	
17.3.3(h)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	
17.3.4 Level 3 requirements				
17.3.4(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	Specific requirement is not mentioned.
17.4 Electronic messaging security				
17.4.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
17.4.2 Level 1 requirements				
17.4.2(a)	INCLUDED	A.10.8 Exchange of information A.12.2 Correct processing in applications	A.10.8.4 Electronic messaging A.12.2.3 Message integrity	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
17.4.2(b)	INCREMENTAL	A.10.8 Exchange of information	A.10.8.1 Information exchange policies and procedures	Information exchange policies, procedures and controls in general. Specific requirement is not mentioned though it could be included in the policies, procedures and controls.
17.4.2(c)	NEW	N.A	N.A	Control of usage of less-secure messaging systems is not mentioned.
17.4.2(d)	INCREMENTAL	A.10.8 Exchange of information A.12.2 Correct processing in applications	A.10.8.4 Electronic messaging A.12.2.3 Message integrity	Implementation of stronger controls when using public networks is not mentioned.
17.4.2(e)	NEW	N.A	N.A	Usage of open standards to prevent and detect spoof emails is not mentioned.
17.4.2(f)	INCREMENTAL	A.10.8 Exchange of information A.12.2 Correct processing in applications	A.10.8.4 Electronic messaging A.12.2.3 Message integrity	Implementation and usage of digital signatures is not mentioned.
17.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
17.4.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
18 Physical and environmental				
18.1 Asset management				
18.1.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.7 Asset management A.9 Physical and environmental security A.14 Business continuity management	N.A	N.A
18.1.2 Level 1 requirements				
18.1.2(a)	INCLUDED	A.7.1 Responsibility for assets	A.7.1.1 Inventory of assets A.7.1.2 Ownership of assets	N.A
18.1.2(b)	INCLUDED	4.2.1 Establish the ISMS	4.2.1(d1) Identify the assets within the scope of the ISMS, and the owners of these assets	N.A
18.1.2(c)	INCREMENTAL	A.9.2 Equipment security A.14 Business continuity management	A.9.2.1 Equipment siting and protection A.9.2.2 Supporting utilities A.9.2.4 Equipment maintenance A.9.2.5 Security of equipment off premises A.14.1.3 Developing and implementing continuity plans including information security	Usage of applicable redundancies is not mentioned.
18.1.2(d)	NEW	N.A	N.A	Protection of cables is mentioned under ISO/IEC 27001:2005 Section A.9.2.3 but disconnection of unused devices is not.
18.1.2(e)	INCLUDED	A.11.3 User responsibilities	A.11.3.2 Unattended user equipment	N.A
18.1.2(f)	INCLUDED	A.11.3 User responsibilities	A.11.3.3 Clear desk and clear screen policy	N.A
18.1.3 Level 2 requirements				
18.1.3(a)	NEW	N.A	N.A	Replacement of assets and decommissioning of out-of-support systems are not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
18.1.3(b)	INCLUDED	A.7.2 Information classification A.9.2 Equipment security	A.7.2.2 Information labeling and handling A.9.2.6 Secure disposal or re-use of equipment	N.A
18.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.2 Off-site movement				
18.2.1 General				
Control Objective	INCLUDED	A.9 Physical and environmental security	N.A	N.A
18.2.2 Level 1 requirements				
18.2.2(a)	INCLUDED	A.9.2 Equipment security	A.9.2.7 Removal of property	N.A
18.2.3 Level 2 requirements				
18.2.3(a)	INCLUDED	A.9.2 Equipment security	A.9.2.7 Removal of property	N.A
18.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.3 Physical access				
18.3.1 General				
Control Objective	INCLUDED	A.8 Human resources security A.9 Physical and environmental security	N.A	N.A
18.3.2 Level 1 requirements				
18.3.2(a)	INCLUDED	A.9.1 Secure areas	A.9.1.1 Physical security perimeter A.9.1.2 Physical entry controls	N.A
18.3.2(b)	INCREMENTAL	A.9.1 Secure areas	A.9.1.1 Physical security perimeter A.9.1.3 Securing offices, rooms and facilities	Physical security elements are present but surveillance is not explicitly mentioned.
18.3.2(c)	INCLUDED	A.9.1 Secure areas	A.9.1.2 Physical entry controls A.9.1.6 Public access, delivery and loading areas	N.A
18.3.2(d)	INCLUDED	A.9.1 Secure areas	A.9.1.1 Physical security perimeter A.9.1.3 Securing offices, rooms and facilities	N.A
18.3.2(e)	INCREMENTAL	A.8.3 Termination or change of employment	A.8.3.3 Removal of access rights	Access granting on a need basis is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
18.3.3 Level 2 requirements				
18.3.3(a)	INCREMENTAL	A.9.1 Secure areas	A.9.1.2 Physical entry controls	Entry controls mentioned in general but not monitoring and storing access logs.
18.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.4 Visitors				
18.4.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.9 Physical and environmental security A.10 Communications and operations management A.11 Access control	N.A	N.A
18.4.2 Level 1 requirements				
18.4.2(a)	INCREMENTAL	A.9.1 Secure areas	A.9.1.1 Physical security perimeter A.9.1.2 Physical entry controls	Escort by authorised personnel to the facility is not mentioned.
18.4.2(b)	INCREMENTAL	A.9.1 Secure areas	A.9.1.1 Physical security perimeter A.9.1.2 Physical entry controls	Having physical security controls in place would imply having requiring pass/badge for access but differentiation between visitors and on-site personnel is not mentioned.
18.4.2(c)	INCLUDED	4.3 Documentation requirements	4.3.3 Control of records	N.A
18.4.2(d)	NEW	N.A	N.A	ISO/IEC 27001:2005 Section 4.3.3 mentioned having a visitors' log but reviewing of such log is not mentioned.
18.4.2(e)	INCREMENTAL	A.10.6 Network security management	A.10.6.1 Network controls	Management and control of networks are mentioned but specific restriction on publicly accessible network points is not.
18.4.3 Level 2 requirements				
18.4.3(a)	INCREMENTAL	A.11.1 Business requirement for access control	A.11.1.1 Access control policy	Management approval not mentioned but access control policy could include such procedures.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
18.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
18.5 Environmental threats and equipment power failures				
18.5.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security	N.A	N.A
18.5.2 Level 1 requirements				
18.5.2(a)	INCLUDED	A.9.1 Secure areas A.9.2 Equipment security	A.9.1.4 Protecting against external and environmental threats A.9.2.1 Equipment siting and protection	N.A
18.5.2(b)	NEW	N.A	N.A	Tamper proofing by external parties is not mentioned.
18.5.2(c)	INCREMENTAL	A.9.2 Equipment security	A.9.2.1 Equipment siting and protection	Protection of equipment from environment threats and hazards is mentioned but not maintaining/monitoring of temperature.
18.5.2(d)	INCREMENTAL	A.9.1 Secure areas	A.9.1.4 Protecting against external and environmental threats	Specific measures against fire are not mentioned.
18.5.2(e)	INCLUDED	A.9.1 Secure areas	A.9.1.4 Protecting against external and environmental threats	N.A
18.5.2(f)	INCREMENTAL	A.9.1 Secure areas	A.9.2.2 Supporting utilities	Protection from power failures mentioned in general but not specific security mechanisms, redundancies, alternative power source and alternative routing.
18.5.2(g)	INCREMENTAL	A.9.1 Secure areas	A.9.2.2 Supporting utilities	Protection from the effects of large amount of systems being turned on is not mentioned.
18.5.2(h)	INCREMENTAL	A.9.1 Secure areas	A.9.2.2 Supporting utilities	Protection from power failures mentioned but not the commensuration of protection with service level commitments.
18.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
18.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
18.6 Physical security review				
18.6.1 General				
Control Objective	INCREMENTAL	4.0 ISMS	N.A	N.A
18.6.2 Level 1 requirements				
18.6.2(a)	INCREMENTAL	4.2.3 Monitor and review the ISMS	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS	Review of ISMS in general. While physical security elements are present, review of physical security controls and procedures is not.
18.6.2(b)	INCREMENTAL	4.2.3 Monitor and review the ISMS	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS	Review of ISMS in general, specific frequency is not mentioned.
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.**				

9.14 Operations

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
19 Operations				
19.1 Operations management policies and procedures				
19.1.1 General				
Control Objective	INCLUDED	4.0 ISMS	N.A	N.A
19.1.2 Level 1 requirements **No applicable Level 1 controls.**				
19.1.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
19.1.3(a)	INCLUDED	4.3.2 Control of documents	4.3.2(b) review and update documents as necessary and re-approve documents 4.3.2(c) ensure that changes and the current revision status of documents are identified 4.3.2(d) ensure that relevant versions of applicable documents are available at points of use 4.3.2(f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification	While not specific to cloud services, this clause is about documentations in general which is adequately covered in ISO/IEC 27001:2005.
19.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
19.2 Documentation of service operations and external dependencies				
19.2.1 General				
Control Objective	INCREMENTAL	4.0 ISMS	N.A	N.A
19.2.2 Level 1 requirements				
19.2.2(a)	INCREMENTAL	4.3.1 General 4.3.2 Control of documents	4.3.1(g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3(c)) 4.3.2(b) review and update documents as necessary and re-approve documents 4.3.2(c) ensure that changes and the current revision status of documents are identified 4.3.2(d) ensure that relevant versions of applicable documents are available at points of use 4.3.2(e) ensure that documents remain legible and readily identifiable 4.3.2(f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification	While not specific to cloud services, this clause is about documentations in general which is adequately covered in ISO/IEC 27001:2005.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
19.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
19.2.4 Level 3 requirements				
19.2.4(a)	INCREMENTAL	4.3.1 General	4.3.1(g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3(c))	External dependencies not explicitly mentioned for documentation.
19.3 Capacity management				
19.3.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management	N.A	N.A
19.3.2 Level 1 requirements				
19.3.2(a)	INCREMENTAL	A.9.2 Equipment security	A.9.2.4 Equipment maintenance	Availability and quality of resources is covered under ISO/IEC 27001:2005 Section A.9.2.4 but not capacity is not.
19.3.2(b)	INCLUDED	A.10.3 System planning and acceptance	A.10.3.1 Capacity management	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(a)	NEW	N.A	N.A	Usage of tools for monitoring critical resources for capacity utilisation is not mentioned.
19.4 Service levels				
19.4.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management	N.A	N.A
19.4.2 Level 1 requirements **No applicable Level 1 controls.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
19.4.3 Level 2 requirements				
19.4.3(a)	INCLUDED	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	N.A
19.4.3(b)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Contractual remedies could be included in agreements though not explicitly mentioned.
19.4.3(c)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Alerts for cloud users could be included in agreements though not explicitly mentioned.
19.4.4 Level 3 requirements				
19.4.4(a)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Redundant network connectivity links could be included in agreements though not explicitly mentioned.
19.4.4(b)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Communication of minimum bandwidth available to users could be included in agreements though not explicitly mentioned.
19.4.4(c)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Communication of available protection measures against malicious attacks could be included in agreements though not explicitly mentioned.
19.4.4(d)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Communication of QoS controls could be included in agreements though not explicitly mentioned.
19.4.4(e)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Bandwidth scalability could be included in agreements though not explicitly mentioned.
19.4.4(f)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Limitations could be included in agreements though not explicitly mentioned.
19.5 Reliability and resiliency				
19.5.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	NEW	4.0 ISMS A.10 Communications and operations management A.14 Business continuity management	N.A	N.A
19.5.2 Level 1 requirements **No applicable Level 1 controls.**				
19.5.3 Level 2 requirements **No applicable Level 2 controls.**				
19.5.4 Level 3 requirements				
19.5.4(a)	INCREMENTAL	4.2.3 Monitor and review the ISMS A.14.1 Information security aspects of business continuity management	4.2.3(b) Undertake regular reviews of the effectiveness of the ISMS A.14.1.5 Testing, maintaining and reassessing business continuity plans	Review of ISMS and BCP in general, specific coverage of review is not mentioned.
19.5.4(b)	NEW	N.A	N.A	Resiliency for storage systems is not mentioned.
19.5.4(c)	NEW	N.A	N.A	Redundancy for SANs is not mentioned.
19.5.4(d)	INCREMENTAL	A.10.6 Network security management	A.10.6.2 Security of network services	Management and control of networks mentioned in general but not specific network equipment and components.
19.5.4(e)	INCREMENTAL	A.10.6 Network security management	A.10.6.2 Security of network services	Management and control of networks mentioned in general but not specifically availability for network equipment and components.
19.5.4(f)	INCREMENTAL	A.10.5 Back-up	A.10.5.1 Information back-up	Back-ups in general, specific use of mirrored or RAID not mentioned.
19.5.4(g)	NEW	N.A	N.A	While back-up is covered generally under A10.5.1, hot spares are not.
19.5.4(h)	INCREMENTAL	4.2.2 Implement and operate the ISMS	4.2.2(h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3(a))	Implementation of capabilities specific for the detection of outages of storage systems is not mentioned.
19.6 Recoverability				
19.6.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCREMENTAL	A.10 Communications and operations management A.14 Business continuity management	N.A	N.A
19.6.2 Level 1 requirements **No applicable Level 1 controls.**				
19.6.3 Level 2 requirements				
19.6.3(a)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1.3 Developing and implementing continuity plans including information security	Plans to be developed for availability mentioned, but usage of primary and alternate sites is not mentioned.
19.6.3(b)	INCREMENTAL	A.10.5 Back-up	A.10.5.1 Information back-up	Back-ups in general are mentioned but the requirement of having adequate point-in-time copies / snapshots is not.
19.6.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
20 Change management				
20.1 Change management process				
20.1.1 General				
Control Objective	INCLUDED	A.6 Organization of information security A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
20.1.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
20.1.2(a)	INCLUDED	A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management A.10.3 System planning and acceptance A.12.4 Security of system files A.12.5 Security in development and support processes	A.10.1.2 Change management A.10.1.4 Separation of development, test and operational facilities A.10.2.3 Managing changes to third party services A.10.3.2 System acceptance A.12.4.1 Control of operational software A.12.4.2 Protection of system test data A.12.5.1 Change control procedures A.12.5.2 Technical review of applications after operating system changes A.12.5.3 Restrictions on changes to software packages	N.A
20.1.3 Level 2 requirements				
20.1.3(a)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery	Procedures for informing affected cloud users could be included in agreements but not explicitly mentioned.
20.1.3(b)	INCLUDED	A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management	A.10.1.2 Change management A.10.2.3 Managing changes to third party services	N.A
20.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
20.2 Backup procedures				
20.2.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management	N.A	N.A
20.2.2 Level 1 requirements				
20.2.2(a)	INCREMENTAL	A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management A.10.5 Back-up	A.10.1.2 Change management A.10.2.3 Managing changes to third party services A.10.5.1 Information back-up	ISO/IEC 27001:2005 covers back-up in general; however, performing backups specifically for systems / applications prior to change is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
20.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
20.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
20.3 Back-out or rollback procedures				
20.3.1 General				
Control Objective	INCREMENTAL	A.6 Organization of information security A.10 Communications and operations management	N.A	N.A
20.3.1 Level 1 requirements **No applicable Level 1 controls.**				
20.3.3 Level 2 requirements				
20.3.3(a)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management A.10.5 Back-up	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery A.10.2.3 Managing changes to third party services A.10.5.1 Information back-up	Back-ups in general are mentioned. Rollback procedures could be included in agreements but not explicitly mentioned.
20.3.4 Level 3 requirements				
20.3.4(a)	INCREMENTAL	A.6.2 External parties A.10.2 Third party service delivery management A.10.5 Back-up	A.6.2.3 Addressing security in third party agreements A.10.2.1 Service delivery A.10.2.3 Managing changes to third party services A.10.5.1 Information back-up	Back-ups in general are mentioned. Alternate recovery options could be included in agreements but not explicitly mentioned.
20.4 Separation of environment				
20.4.1 General				
Control Objective	INCLUDED	A.10 Communications and operations management	N.A	N.A
20.4.2 Level 1 requirements				
20.4.2(a)	INCLUDED	A.10.1 Operational procedures and responsibilities	A.10.1.4 Separation of development, test and operational facilities	N.A
20.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
20.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
20.5 Patch management procedures				
20.5.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
20.5.2 Level 1 requirements				
20.5.2(a)	INCREMENTAL	A.10.2 Third party service delivery management	A.10.2.1 Service delivery A.10.2.3 Managing changes to third party services	Implementation of patch management procedures is not mentioned.
20.5.2(b)	INCREMENTAL	A.10.2 Third party service delivery management	A.10.2.1 Service delivery	Implementation of a process to manage systems that have been dormant/offline is not mentioned.
20.5.3 Level 2 requirements				
20.5.3(a)	INCREMENTAL	A.12.6 Technical Vulnerability Management	A.12.6.1 Control of technical vulnerabilities	Identification of vulnerabilities is mentioned but not the assignment of risk ratings.
20.5.3(b)	NEW	N.A	N.A	Prioritization and definition of specific periods to application of security patches is not mentioned.
20.5.3(c)	NEW	N.A	N.A	ISO/IEC 27001:2005 Section A.10.1.4 covered the separation of test and production environments but testing of patches is not mentioned.
20.5.3(d)	INCREMENTAL	A.10.2 Third party service delivery management	A.10.2.1 Service delivery	Implementation of a process to manage systems that have been dormant / offline for over 30 days is not mentioned.
20.5.4 Level 3 requirements				
20.5.4(a)	NEW	N.A	N.A	Patch management procedures are not mentioned.

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

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
21 Business continuity planning (BCP) and disaster recovery (DR)				
21.1 BCP framework				
21.1.1 General				
Control Objective	INCLUDED	4.0 ISMS A.7 Asset management A.14 Business continuity management	N.A	N.A
21.1.2 Level 1 requirements				
21.1.2(a)	INCLUDED	4.2.1 Establish the ISMS A.7.2 Information classification	4.2.1(d) Identify the risks. A.7.2.1 Classification guidelines	N.A.
21.1.2(b)	INCLUDED	4.2.1 Establish the ISMS A.14.1 Information security aspects of business continuity management	4.2.1(d) Identify the risks. A.14.1.2 Business continuity and risk assessment	N.A
21.1.2(c)	INCLUDED	4.2.1 Establish the ISMS A.14.1 Information security aspects of business continuity management	4.2.1(d) Identify the risks A.14.1.2 Business continuity and risk assessment	N.A
21.1.2(d)	INCLUDED	4.2.1 Establish the ISMS A.14.1 Information security aspects of business continuity management	4.2.1(d) Identify the risks A.14.1.2 Business continuity and risk assessment	N.A
21.1.2(e)	INCLUDED	4.2.1 Establish the ISMS A.14.1 Information security aspects of business continuity management	4.2.1(e) Analyze and evaluate the risks A.14.1.3 Developing and implementing continuity plans including information security	N.A
21.1.2(f)	INCLUDED	4.2.1 Establish the ISMS A.14.1 Information security aspects of business continuity management	4.2.1(e) Analyze and evaluate the risks A.14.1.4 Business continuity planning framework	N.A
21.1.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
21.1.3(a)	INCLUDED	A.14.1 Information security aspects of business continuity management	A.14.1.3 Developing and implementing continuity plans including information security	Recovery time objective (RTO) is not explicitly mentioned, but required time scale for recovery is.
21.1.3(b)	INCLUDED	A.14.1 Information security aspects of business continuity management	A.14.1.3 Developing and implementing continuity plans including information security	Recovery point objective (RPO) is not explicitly mentioned, but required time scale for recovery is.
21.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
21.2 BCP and DR plans				
21.2.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.9 Physical and environmental security A.14 Business continuity management	N.A	N.A
21.2.2 Level 1 requirements				
21.2.2(a)	INCREMENTAL	4.2.1 Establish the ISMS A.14.1 Information security aspects of business continuity management	4.2.1(d) Identify the risks A.14.1.2 Business continuity and risk assessment A.14.1.4 Business continuity planning framework	Disaster recovery is not mentioned in ISO/IEC 27001:2005 though elements of it can be found in business continuity planning-related clauses.
21.2.2(b)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1.1 Including information security in the business continuity management process A.14.1.3 Developing and implementing continuity plans including information security A.14.1.4 Business continuity planning framework	Roles and responsibilities not explicitly mentioned but could be included in the business continuity planning (BCP) / disaster recovery (DR) planning process and framework.
21.2.2(c)	INCLUDED	A.14.1 Information security aspects of business continuity management	A.14.1.1 Including information security in the business continuity management process A.14.1.3 Developing and implementing continuity plans including information security	N.A
21.2.2(d)	INCLUDED	A.9.2 Equipment security A.14.1 Information security aspects of business continuity management	A.9.2.1 Equipment siting and protection A.14.1.2 Business continuity and risk assessment A.14.1.3 Developing and implementing continuity plans including information security	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
21.2.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
21.2.4 Level 3 requirements				
21.2.4(a)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1.3 Developing and implementing continuity plans including information security	Implementation of rapid operational and backup capabilities is not mentioned.
21.2.4(b)	INCLUDED	A.14.1 Information security aspects of business continuity management	A.14.1.2 Business continuity and risk assessment	N.A
21.2.4(c)	INCLUDED	A.14.1 Information security aspects of business continuity management	A.14.1.3 Developing and implementing continuity plans including information security	N.A
21.2.4(d)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1.3 Developing and implementing continuity plans including information security	Set up of alternate recovery site is not mentioned.
21.3 BCP and DR testing				
21.3.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance A.14 Business continuity management	N.A	Disaster recovery is not mentioned in ISO/IEC 27001:2005.
21.3.2 Level 1 requirements				
21.3.2(a)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1.5 Testing, maintaining and reassessing business continuity plans	Disaster recovery is not mentioned in ISO/IEC 27001:2005 though elements of it can be found in business continuity planning-related clauses.
21.3.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
21.3.4 Level 3 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
21.3.4(a)	INCREMENTAL	A.14.1 Information security aspects of business continuity management	A.14.1.5 Testing, maintaining and reassessing business continuity plans	Disaster recovery is not mentioned in ISO/IEC 27001:2005 though elements of it can be found in business continuity planning-related clauses. Specific frequency for testing is not mentioned. Specific test case scenarios are also not mentioned.
21.3.4(b)	INCLUDED	A.10.5 Back-up	A.10.5.1 Information back-up	N.A
21.3.4(c)	INCLUDED	A.10.5 Back-up A.12.3 Cryptographic controls	A.10.5.1 Information back-up A.12.3.1 Policy on the use of cryptographic controls	N.A

9.17 Cloud services administration

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.1 Privilege account creation				
22.1.1 General				
Control Objective	INCREMENTAL	A.11 Access control	N.A	N.A
22.1.2 Level 1 requirements				
22.1.2(a)	INCLUDED	A.11.2 User access management A.11.5 Operating system access control	A.11.2.1 User registration A.11.5.2 User identification and authentication	N.A
22.1.2(b)	INCLUDED	A.11.2 User access management A.11.5 Operating system access control	A.11.2.1 User registration A.11.5.2 User identification and authentication	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.1.2(c)	INCREMENTAL	A.11.1 Business requirement for access control A.11.2 User access management	A.11.1.1 Access control policy A.11.2.1 User registration	Access granting procedures could be included in access control policy. While this clause has cloud-specific components in it, it has the same context as traditional ISMS and technology environments.
22.1.2(d)	NEW	N.A	N.A	Privileged accounts are not mentioned.
22.1.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
22.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.2 Generation of administrator passwords				
22.2.1 General				
Control Objective	INCLUDED	A.11 Access control	N.A	Specific password criteria are not mentioned in ISO/IEC 27001:2005.
22.2.2 Level 1 requirements				
22.2.2(a)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords are mentioned in general. Specific password criteria are not mentioned.
22.2.2(b)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords are mentioned in general.
22.2.2(c)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords are mentioned in general.
22.2.3 Level 2 requirements				
22.2.3(a)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords are mentioned in general. Specific password criteria are not mentioned.
22.2.3(b)	INCREMENTAL	A.11.5 Operating system access control	A.11.5.2 User identification and authentication	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
22.2.3(c)	INCREMENTAL	A.11.5 Operating system access control	A.11.5.2 User identification and authentication	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
22.2.4 Level 3 requirements **The requirements are the same as those in Level 2.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.3 Administrator access review and revocation				
22.3.1 General				
Control Objective	INCREMENTAL	A.8 Human resources security A.10 Communications and operations management A.11 Access control	N.A	N.A
22.3.2 Level 1 requirements				
22.3.2(a)	INCLUDED	A.8.3 Termination or change of employment	A.8.3.3 Removal of access rights	N.A
22.3.2(b)	INCLUDED	A.11.2 User access management	A.11.2.4 Review of user access rights	N.A
22.3.2(c)	INCREMENTAL	A.11.2 User access management	A.11.2.4 Review of user access rights	Removal or disabling of inactive accounts could be part of the review process. Specific frequency is not mentioned.
22.3.2(d)	INCLUDED	A.8.3 Termination or change of employment A.11.2 User access management	A.8.3.3 Removal of access rights A.11.2.4 Review of user access rights	N.A
22.3.3 Level 2 requirements				
22.3.3(a)	INCLUDED	A.10.10 Monitoring A.11.2 User access management	A.10.10.1 Audit logging A.11.2.2 Privilege management	N.A
22.3.3 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.4 Account lockout				
22.4.1 General				
Control Objective	NEW	N.A	N.A	Account lockout is not mentioned in ISO/IEC 27001:2005.
22.4.2 Level 1 requirements				
22.4.2(a)	NEW	N.A	N.A	Account lockout and lockout criteria are not mentioned in ISO/IEC 27001:2005.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.4.2(b)	NEW	N.A	N.A	Account lockout and lockout duration are not mentioned in ISO/IEC 27001:2005.
22.4.3 Level 2 requirements				
22.4.3(a)	NEW	N.A	N.A	Account lockout and lockout duration are not mentioned in ISO/IEC 27001:2005.
22.4.3 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.5 Password change				
22.5.1 General				
Control Objective	INCREMENTAL	A.11 Access control	N.A	N.A
22.5.2 Level 1 requirements				
22.5.2(a)	NEW	N.A	N.A	Enforcement of compulsory password change is not mentioned.
22.5.2(b)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Password history requirement is not mentioned.
22.5.3 Level 2 requirements				
22.5.3(a)	NEW	N.A	N.A	Two-factor authentication (2FA) and token change procedures are not mentioned.
22.5.3 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.6 Password reset and first logon				
22.6.1 General				
Control Objective	INCLUDED	A.11 Access control	N.A	N.A
22.6.2 Level 1 requirements				
22.6.2(a)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Generation of unique passwords and mandatory password change upon first login are not mentioned.
22.6.2(b)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Verification of identity prior to changing password is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.6.2(c)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Management approval for password reset is not mentioned.
22.6.2(d)	NEW	N.A	N.A	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
22.6.3 Level 2 requirements				
22.6.3(a)	INCREMENTAL	A.11.5 Operating system access control	A.11.5.3 Password management system	Password management system is mentioned in general, not specific for generation, custody and distribution of service management passwords. Split control and out-of-band mechanism are not mentioned.
22.6.4 Level 3 requirements				
22.6.4(a)	INCREMENTAL	A.11.5 Operating system access control	A.11.5.3 Password management system	Password management system is mentioned in general, the need for having two halves of a password, with each half given to different person, is not mentioned.
22.7 Administrator access security				
22.7.1 General				
Control Objective	INCREMENTAL	A.11 Access control	N.A	N.A
22.7.2 Level 1 requirements				
22.7.2(a)	INCLUDED	A.11.4 Network access control	A.11.4.3 Equipment identification in networks	While this clause has cloud-specific components in it, its purpose is covered is covered under ISO/IEC 27001:2005 Section A.11.4.3.
22.7.2(b)	INCLUDED	A.11.4 Network access control	A.11.4.3 Equipment identification in networks A.11.4.6 Network connection control	N.A
22.7.2(c)	INCLUDED	A.11.2 User access management	A.11.2.2 Privilege management	N.A
22.7.2(d)	NEW	N.A	N.A	Explicit approval for enablement of administrative rights is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.7.2(e)	INCREMENTAL	A.11.2 User access management	A.11.2.2 Privilege management	Role-based access control (RBAC) mechanisms are not mentioned.
22.7.3 Level 2 requirements				
22.7.3(a)	INCREMENTAL	A.11.4 Network access control	A.11.4.3 Equipment identification in networks	Bastion hosts are not mentioned.
22.7.4 Level 3 requirements				
22.7.4(a)	INCREMENTAL	A.11.6 Application and information access control	A.11.6.1 Information access restriction	Control of access in accordance with the defined access control policy in general. Usage of privilege access management tools is not mentioned.
22.8 Administrator access logs				
22.8.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management	N.A	N.A
22.8.2 Level 1 requirements				
22.8.2(a)	NEW	N.A	N.A	Procedure to review administrator activities is not mentioned.
22.8.3 Level 2 requirements				
22.8.3(a)	INCREMENTAL	A.10.10 Monitoring	A.10.10.3 Protection of log information	Protection of logs in general, not specifically against tampering by the administrator. Automatic alerting and escalation for violations to access control policies are also not mentioned.
22.8.4 Level 3 requirements				
22.8.4(a)	INCLUDED	A.10.10 Monitoring	A.10.10.4 Administrator and operator logs	N.A
22.9 Session management				
22.9.1 General				
Control Objective	INCREMENTAL	A.11.5 Operating system access control	N.A	N.A
22.9.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.9.2(a)	INCLUDED	A.11.5 Operating system access control	A.11.5.5 Session time-out	N.A
22.9.2(a)	INCREMENTAL	A.11.5 Operating system access control	A.11.5.5 Session time-out	Requirement to re-enter password after session idle is not mentioned. Specific period of idling is also not mentioned.
22.9.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
22.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.10 Segregation of duties				
22.10.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.11 Access control	N.A	N.A
22.10.2 Level 1 requirements				
22.10.2(a)	INCREMENTAL	A.10.1 Operational procedures and responsibilities A.11.2 User access management	A.10.1.3 Segregation of duties A.11.2.4 Review of user access rights	Specific frequency of review is not mentioned.
22.10.2(b)	INCREMENTAL	A.10.1 Operational procedures and responsibilities A.11.2 User access management	A.10.1.4 Separation of development, test and operational facilities A.10.4.1 Controls against malicious code A.11.2.2 Privilege management	Movement of object codes between environments is not mentioned.
22.10.2(c)	INCREMENTAL	A.10.1 Operational procedures and responsibilities A.11.1 Business requirement for access control A.11.2 User access management	A.10.1.4 Separation of development, test and operational facilities A.11.1.1 Access control policy A.11.2.2 Privilege management	Separation of environments mentioned but not restriction of access to backup and production systems.
22.10.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.10.3(a)	INCREMENTAL	A.11.2 User access management	A.11.2.4 Review of user access rights	Specific frequency of review is not mentioned.
22.10.4 Level 3 requirements				
22.10.4(a)	INCREMENTAL	A.11.2 User access management	A.11.2.4 Review of user access rights	Specific frequency of review is not mentioned.
22.11 Secure transmission of access credentials				
22.11.1 General				
Control Objective	NEW	N.A	N.A	N.A
22.11.2 Level 1 requirements				
22.11.2(a)	NEW	N.A	N.A	Usage of no clear-text protocols for administrative access is not mentioned in ISO/IEC 27001:2005.
22.11.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
22.11.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
22.12 Third party administrative access				
22.12.1 General				
Control Objective	INCLUDED	A.6 Organization of information security A.8 Human resources security A.10 Communications and operations management A.11 Access control	N.A	N.A
22.12.2 Level 1 requirements				
22.12.2(a)	INCREMENTAL	A.8.1 Prior to employment A.11.1 Business requirement for access control A.11.2 User access management	A.8.1.1 Roles and responsibilities A.11.1.1 Access control policy A.11.2.2 Privilege management	Granting access on a need-to-have basis is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.12.2(b)	INCLUDED	A.6.2 External parties A.10.2 Third party service delivery management	A.6.2.1 Identification of risks related to external parties A.6.2.3 Addressing security in third party agreements A.10.2.2 Monitoring and review of third party services	N.A
22.12.3 Level 2 requirements				
22.12.3(a)	INCLUDED	A.8.3 Termination or change of employment A.10.2 Third party service delivery management A.11.4 Network access control	A.8.3.3 Removal of access rights A.10.2.2 Monitoring and review of third party services A.11.4.2 User authentication for external connections	N.A
22.12.4 Level 3 requirements				
22.12.4(a)	INCREMENTAL	A.10.2 Third party service delivery management	A.10.2.2 Monitoring and review of third party services	Requirement of direct supervision by CSP's relevant personnel is not mentioned.
22.13 Service and application accounts				
22.13.1 General				
Control Objective	INCREMENTAL	A.11 Access control A.12 Information systems acquisition, development and maintenance	N.A	N.A
22.13.2 Level 1 requirements				
22.13.2(a)	INCREMENTAL	A.11.2 User access management	A.11.2.1 User registrationA.11.2.2 Privilege management	Service and application accounts not explicitly mentioned.
22.13.3 Level 2 requirements				
22.13.3(a)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Managing and control of allocation of password in general. Implementation of either control for the creation of service accounts is not mentioned.
22.13.3(b)	INCREMENTAL	A.11.2 User access management A.11.5 Operating system access control	A.11.2.2 Privilege management A.11.5.5 Session time-out	Privilege management and session management in general, prohibition of caching or storing of sensitive session parameters, cookies or similar on local machines is not explicitly mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
22.13.3(c)	INCREMENTAL	A.11.2 User access management A.11.5 Operating system access control	A.11.2.2 Privilege management A.11.5.5 Session time-out	Privilege management and session management in general, prohibition of simultaneous logins is not explicitly mentioned.
22.13.3(d)	INCREMENTAL	A.11.2 User access management	A.11.2.2 Privilege management	Privilege management in general, prohibition of console login access is not explicitly mentioned.
22.13.3(e)	INCREMENTAL	A.12.1 Security requirements of information systems	A.12.1.1 Security requirements analysis and specification	Including security requirements for new systems mentioned in general, but not specifically for systems to be used in the cloud environment.
22.13.4 Level 3 requirements				
22.13.4(a)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Procedures and frequency for change of service account passwords are not mentioned.

9.18 Cloud user access

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
23 Cloud user access				
23.1 User access registration				
23.1.1 General				
Control Objective	INCLUDED	A.8 Human resources security A.11 Access control	N.A	N.A
23.1.2 Level 1 requirements				
23.1.2(a)	INCLUDED	A.11.2 User access management A.11.5 Operating system access control	A.11.2.1 User registration A.11.5.2 User identification and authentication	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
23.1.2(b)	INCLUDED	A.8.1 Prior to employment A.11.1 Business requirement for access control A.11.2 User access management	A.8.1.1 Roles and responsibilities A.11.1.1 Access control policy A.11.2.2 Privilege management	N.A
23.1.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
23.1.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.2 User access security				
23.2.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.11 Access control	N.A	N.A
23.2.2 Level 1 requirements				
23.2.2(a)	INCREMENTAL	A.11.2 User access management	A.11.2.1 User registration	Enforcement of documented approval from authorised personnel not mentioned.
23.2.2(b)	INCLUDED	A.10.10 Monitoring	A.10.10.3 Protection of log information	N.A
23.2.2(c)	NEW	N.A	N.A	"Deny-all" setting is not mentioned.
23.2.2(d)	INCLUDED	A.10.9 Electronic commerce services	A.10.9.3 Publicly available information	While the restriction of write / modify access is not explicitly mentioned, the protection of the integrity if the information could imply the existence of controls for such controls.
23.2.2(e)	NEW	N.A	N.A	Implementation of anti-bot controls is not mentioned.
23.2.3 Level 2 requirements				
23.2.3(a)	NEW	N.A	N.A	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
23.2.4 Level 3 requirements				
23.2.4(a)	NEW	N.A	N.A	Identity management is not mentioned in ISO/IEC 27001:2005.
23.3 User access password				
23.3.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	INCLUDED	A.11 Access control	N.A	N.A
23.3.2 Level 1 requirements				
23.3.2(a)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Specific password criteria are not mentioned in ISO/IEC 27001:2005.
23.3.2(b)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords are mentioned in general.
23.3.2(c)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords are mentioned in general.
23.3.3 Level 2 requirements				
23.3.3(a)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Specific password criteria are not mentioned in ISO/IEC 27001:2005.
23.3.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.4 User account lockout				
23.4.1 General				
Control Objective	NEW	N.A	N.A	Account lockout is not mentioned in ISO/IEC 27001:2005.
23.4.2 Level 1 requirements				
23.4.2(a)	NEW	N.A	N.A	Account lockout criteria are not mentioned in ISO/IEC 27001:2005.
23.4.2(b)	NEW	N.A	N.A	Account lockout duration is not mentioned in ISO/IEC 27001:2005.
23.4.3 Level 2 requirements				
23.4.3(a)	NEW	N.A	N.A	Account lockout criteria are not mentioned in ISO/IEC 27001:2005.
23.4.3(b)	NEW	N.A	N.A	Account lockout duration is not mentioned in ISO/IEC 27001:2005.
23.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.5 User password reset and 1st logon change				
23.5.1 General				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
Control Objective	NEW	A.11 Access control	N.A	N.A
23.5.2 Level 1 requirements				
23.5.2(a)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Generation of unique passwords and mandatory password change upon first login are not mentioned.
23.5.2(b)	INCREMENTAL	A.11.2 User access management	A.11.2.3 User password management	Verification of user identity in the event of a password reset is not mentioned.
23.5.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
23.5.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.6 Password protection				
23.6.1 General				
Control Objective	INCREMENTAL	A.10 Communications and operations management A.12 Information systems acquisition, development and maintenance	N.A	N.A
23.6.2 Level 1 requirements				
23.6.2(a)	INCREMENTAL	A.10.8 Exchange of information A.12.3 Cryptographic controls	A.10.8.1 Information exchange policies and procedures A.12.3.1 Policy on the use of cryptographic controls	Rendering passwords unreadable during transmission not explicitly mentioned.
23.6.2(b)	INCREMENTAL	A.10.8 Exchange of information A.12.3 Cryptographic controls	A.10.8.1 Information exchange policies and procedures A.12.3.1 Policy on the use of cryptographic controls	Information exchange policies, procedures and controls in general. Usage of encrypted channels could be included in exchange policies.
23.6.2(c)	NEW	N.A	N.A	Password storage is not mentioned in ISO/IEC 27001:2005.
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.**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
23.7 User session management				
23.7.1 General				
Control Objective	INCREMENTAL	A.8 Human resources security A.10 Communications and operations management A.11 Access control A.12 Information systems acquisition, development and maintenance	N.A	N.A
23.7.2 Level 1 requirements				
23.7.2(a)	INCLUDED	A.11.5 Operating system access control	A.11.5.5 Session time-out	N.A
23.7.2(b)	INCREMENTAL	A.11.5 Operating system access control	A.11.5.5 Session time-out	Requirement to re-enter password after session idle is not mentioned. Specific period of idling is also not mentioned.
23.7.2(c)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.1 Policy on the use of cryptographic controls	Implementation of cryptographically strong session identifiers is not mentioned.
23.7.3 Level 2 requirements				
23.7.3(a)	INCLUDED	A.8.3 Termination or change of employment A.10.2 Third party service delivery management A.11.4 Network access control	A.8.3.3 Removal of access rights A.10.2.2 Monitoring and review of third party services A.11.4.2 User authentication for external connections	N.A
23.7.4 Level 3 requirements				
23.7.4(a)	INCLUDED	A.11.5 Operating system access control	A.11.5.6 Limitation of connection time	N.A
23.8 Change of cloud user's administrator details notification				
23.8.1 General				
Control Objective	NEW	N.A	N.A	N.A
23.8.2 Level 1 requirements **No applicable Level 1 controls**				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
23.8.3 Level 2 requirements				
23.8.3(a)	NEW	N.A	N.A	Alert for change in administrator details is not mentioned in ISO/IEC 27001:2005.
23.8.3(b)	NEW	N.A	N.A	Effecting of change in administrator details is not mentioned in ISO/IEC 27001:2005.
23.8.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.9 Self-service portal creation and management of user accounts				
23.9.1 General				
Control Objective	INCREMENTAL	A.11 Access control	N.A	N.A
23.9.2 Level 1 requirements				
23.9.2(a)	INCREMENTAL	A.11.3 User responsibilities	A.11.3.1 Password use	Good security practices for passwords mentioned in general. Specific password criteria are not mentioned in ISO/IEC 27001:2005.
23.9.2(b)	INCLUDED	A.11.1 Business requirement for access control	A.11.2.1 User registration A.11.2.2 Privilege management	N.A
23.9.3 Level 2 requirements				
23.9.3(a)	INCLUDED	A.11.2 User access management	A.11.2.1 User registration	N.A
23.9.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
23.10 Communication with cloud users				
23.10.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.8 Human resources security	N.A	N.A
23.10.2 Level 1 requirements				
23.10.2(a)	NEW	N.A	N.A	Security of notifications is not mentioned.
23.10.3 Level 2 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
23.10.3(a)	INCREMENTAL	4.2.2 Implement and operate the ISMS A.8.2 During employment	4.2.2(e) Implement training and awareness programs (see 5.2.2) A.8.2.2 Information security awareness, education and training	Specific topics for user education are not mentioned.
23.10.4 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 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24 Tenancy and customer isolation				
24.1 Multi tenancy				
24.1.1 General				
Control Objective	NEW	A.11 Access control	N.A	N.A
24.1.2 Level 1 requirements				
24.1.2(a)	INCLUDED	A.11.4 Network access control	A.11.4.5 Segregation in networks	N.A
24.1.2(b)	INCLUDED	A.11.1 Business requirement for access control A.11.2 User access management	A.11.1.1 Access control policy A.11.2.2 Privilege management	N.A
24.1.2(c)	INCREMENTAL	A.11.4 Network access control	A.11.4.5 Segregation in networks	Segregation of networks in general is mentioned. However, virtual machines are not mentioned in ISO/IEC 27001:2005.
24.1.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
24.1.4 Level 3 requirements				
24.1.4(a)	NEW	N.A	N.A	Implementation of monitoring mechanisms to detect the specified requirement is not mentioned.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24.1.4(b)	NEW	N.A	N.A	Virtual hosts are not mentioned in ISO/IEC 27001:2005.
24.1.4(c)	NEW	N.A	N.A	Virtual hosts are not mentioned in ISO/IEC 27001:2005.
24.2 Supporting infrastructure segmentation				
24.2.1 General				
Control Objective	INCREMENTAL	A.11 Access control	N.A	N.A
24.2.2 Level 1 requirements **No applicable Level 1 controls**				
24.2.3 Level 2 requirements				
24.2.3(a)	INCREMENTAL	A.11.4 Network access control	A.11.4.5 Segregation in networks	Network segregation in general and not specific to the separation of authentication sources for cloud service components.
24.2.3(b)	INCLUDED	A.11.4 Network access control	A.11.4.5 Segregation in networks A.11.4.6 Network connection control	While this clause has cloud-specific components in it, its purpose is covered is covered under ISO/IEC 27001:2005 Sections A.11.4.5 and A.11.4.6.
24.2.3(c)	INCREMENTAL	A.11.4 Network access control	A.11.4.5 Segregation in networks A.11.4.6 Network connection control	Two-factor authentication (2FA) is not mentioned in ISO/IEC 27001:2005.
24.2.4 Level 3 requirements				
24.2.4(a)	INCLUDED	A.11.4 Network access control	A.11.4.5 Segregation in networks	While this clause has cloud-specific components in it, its purpose is covered is covered under ISO/IEC 27001:2005 Section A.11.4.5.
24.3 Network protection				
24.3.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security A.10 Communications and operations management A.11 Access control	N.A	N.A
24.3.2 Level 1 requirements				

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24.3.2(a)	INCLUDED	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.7 Network routing control	N.A
24.3.2(b)	INCLUDED	A.11.4 Network access control	A.11.4.5 Segregation in networks A.11.4.6 Network connection control A.11.4.7 Network routing control	N.A
24.3.2(c)	INCLUDED	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.6 Network connection control A.11.4.7 Network routing control	N.A
24.3.2(d)	INCREMENTAL	A.10.6 Network security management	A.10.6 Network security management (all)	Comparison of network configurations against standards not mentioned.
24.3.2(e)	NEW	N.A	N.A	Review of network environment is not mentioned.
24.3.2(f)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(d) Identify the risks	Identification of risks related to data flow network architecture not mentioned.
24.3.2(g)	INCLUDED	A.11.1 Business requirement for access control A.11.4 Network access control A.11.6 Application and information access control	A.11.1.1 Access control policy A.11.4.1 Policy on use of network services A.11.6.1 Information access restriction	N.A
24.3.2(h)	INCLUDED	A.10.8 Exchange of information A.11.4 Network access control	A.10.8.1 Information exchange policies and procedures A.10.8.2 Exchange agreements A.11.4.1 Policy on use of network services	N.A
24.3.2(i)	INCLUDED	A.11.4 Network access control	A.11.4.7 Network routing control	N.A
24.3.2(j)	NEW	N.A	N.A	Multi-factor authentication is not mentioned in ISO/IEC 27001:2005.
24.3.2(k)	NEW	N.A	N.A	Virtualisation layer is not mentioned in ISO/IEC 27001:2005.

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24.3.2(l)	NEW	N.A	N.A	Multi-factor authentication and split control authentication are not mentioned in ISO/IEC 27001:2005.
24.3.2(m)	INCLUDED	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.6 Network connection control	N.A
24.3.3 Level 2 requirements				
24.3.3(a)	INCLUDED	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.6 Network connection control	N.A
24.3.3(b)	INCLUDED	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.6 Network connection control	N.A
24.3.3(c)	INCREMENTAL	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.6 Network connection control	Prohibition of direct public access to systems hosting sensitive data not explicitly mentioned.
24.3.3(d)	NEW	N.A	N.A	Stateful inspection is not mentioned in ISO/IEC 27001:2005.
24.3.3(e)	NEW	N.A	N.A	Internal IP address disclosure is not mentioned in ISO/IEC 27001:2005.
24.3.3(f)	INCLUDED	A.10.6 Network security management A.11.4 Network access control	A.10.6 Network security management (all) A.11.4.6 Network connection control	N.A
24.3.4 Level 3 requirements				
24.3.4(a)	INCLUDED	A.9.1 Secure areas A.10.6 Network security management A.11.4 Network access control	A.9.1.3 Securing offices, rooms and facilities A.10.6 Network security management (all) A.11.4.6 Network connection control	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24.4 Virtualisation				
24.4.1 General				
Control Objective	INCREMENTAL	4.0 ISMS A.9 Physical and environmental security	N.A	Virtualisation is not mentioned in ISO/IEC 27001:2005.
24.4.2 Level 1 requirements				
24.4.2(a)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(d) Identify the risks	Specific VM-related features, risks and configurations are not mentioned in ISO/IEC 27001:2005.
24.4.2(b)	INCREMENTAL	4.2.1 Establish the ISMS	4.2.1(d) Identify the risks 4.2.1(f) Identify and evaluate options for the treatment of risks	Risk assessment and treatment specifically for virtualised IT systems and services are not mentioned.
24.4.2(c)	INCREMENTAL	A.9.2 Equipment security	A.9.2.5 Security of equipment off premises A.9.2.7 Removal of property	Encryption of VMs is not mentioned is ISO/IEC 27001:2005.
24.4.3 Level 2 requirements **The requirements are the same as those in Level 1.**				
24.4.4 Level 3 requirements **The requirements are the same as those in Level 2.**				
24.5 Storage area networks (SAN)				
24.5.1 General				
Control Objective	NEW	A.9 Physical and environmental security A.10 Communications and operations management A.11 Access control A.12 Information systems acquisition, development and maintenance	N.A	N.A
24.5.2 Level 1 requirements				
24.5.2(a)	INCLUDED	A.11.1 Business requirement for access control A.11.4 Network access control	A.11.1.1 Access control policy A.11.4.1 Policy on use of network services A.11.4.6 Network connection control	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24.5.2(b)	INCREMENTAL	A.9.2 Equipment security	A.9.2.4 Equipment maintenance	Implementation of process for propagating all configuration changes is not mentioned.
24.5.3 Level 2 requirements				
24.5.3(a)	INCLUDED	A.11.4 Network access control	A.11.4.1 Policy on use of network services A.11.4.6 Network connection control	N.A
24.5.3(b)	INCLUDED	A.11.4 Network access control	A.11.4.4 Remote diagnostic and configuration port protection	N.A.
24.5.3(c)	NEW	N.A	N.A	Mutual authentication between devices is not mentioned in ISO/IEC 27001:2005.
24.5.3(d)	INCLUDED	A.11.1 Business requirement for access control A.11.4 Network access control	A.11.1.1 Access control policy A.11.4.1 Policy on use of network services A.11.4.6 Network connection control	N.A
24.5.3(e)	NEW	N.A	N.A	Automatic replication is not mentioned in ISO/IEC 27001:2005.
24.5.4 Level 3 requirements				
24.5.4(a)	NEW	N.A	N.A	Hard zones are not mentioned in ISO/IEC 27001:2005.
24.5.4(b)	NEW	N.A	N.A	Logical Unit Numbers (LUN) masking is not mentioned in ISO/IEC 27001:2005.
24.5.4(c)	INCLUDED	A.10.8 Exchange of information A.12.3 Cryptographic controls	A.10.8.1 Information exchange policies and procedures A.10.8.5 Business information systems A.12.3.1 Policy on the use of cryptographic controls	N.A
24.5.4(d)	NEW	N.A	N.A	Option for customers to maintain control of the encryption keys is not mentioned.
24.6 Data segregation				
24.6.1 General				
Control Objective	INCREMENTAL	A.9 Physical and environmental security A.12 Information systems acquisition, development and maintenance	N.A	N.A

MTCS clause	Gaps	Reference to matching ISO/IEC 27001:2005 clauses	Reference to matching ISO/IEC 27001:2005 subclauses	Remarks on identified gaps
24.6.2 Level 1 requirements **No applicable Level 1 controls**				
24.6.3 Level 2 requirements				
24.6.3(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	Logical segregation for data access, logs, and encryption keys is not mentioned.
24.6.3(b)	INCREMENTAL	A.9.2 Equipment security	A.9.2.5 Security of equipment off premises	Security of equipment off premises in general.
24.6.4 Level 3 requirements				
24.6.4(a)	INCREMENTAL	A.12.3 Cryptographic controls	A.12.3.2 Key management	Allowing cloud user control of encryption not mentioned.
24.6.4(b)	NEW	N.A	N.A	Segregation of back-ups by users is not mentioned in ISO/IEC 27001:2005.

<End of Gap Analysis Report>