INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Alignment of MTCS to Healthcare IT Security Policy & Standards

Gap Analysis Report

Version : 1.0, Apr 2016

Document Change Log

Document Name: Alignment of MTCS to Healthcare IT Security Policy & Standards – Gap Analysis Report

Revision Date	Version	Updated By	Description
April 2016	Version 1.0	IDA	Initial Release

Contents

FOREWORD

The MTCS for Healthcare Working Group is initiated by the National Cloud Computing Office at IDA to assist in the preparation of the Alignment of MTCS to Healthcare IT Security Policy & Standards - Gap Analysis Report. It comprises the following security, network and infrastructure specialists.

Chairperson:	Karen Wong
Deputy Chair:	Tao Yao Sing
Secretary:	Julian Loh
Members:	Prashant Agrawal
	Chua Kim Chuan
	Francis Fan
	Sydney Lim
	Gregory Malewski

The organizations in which the experts of the Working Group (WG) are affiliated with are:

Ministry of Health, Singapore

MOH Holdings Pte Ltd, Singapore

Integrated Health and Information Systems Pte Ltd, Singapore

Infocomm Development Authority of Singapore

Disclaimer

The information provided in the Alignment of MTCS to Healthcare IT Security Policy & Standards - Gap Analysis Report is for general information purposes only. The Alignment of MTCS to Healthcare IT Security Policy & Standards - Gap Analysis Report is provided "AS IS" without any express or implied warranty of any kind. Whilst the Working Group (defined above), 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 Alignment of MTCS to Healthcare IT Security Policy & Standards - Gap Analysis Report. The Working Group and IDA are entitled to add, delete or change any information in the Alignment of MTCS to Healthcare IT Security Policy & Standards - Gap Analysis Report at any time at their absolute discretion without giving any reasons.

1. INTRODUCTION

Since the launch of MTCS standard in November 2013, a number of related developments has taken place. As part of our initiative to significantly increase adoption in specific industry verticals (such as healthcare) where cloud security remains a key impediment, it is important to align MTCS standard to the Ministry of Health's Healthcare IT Security Policy & Standards (HITSecP). The objective is to enable MTCS certified Cloud Service Providers (CSPs) to provide HITSecP compliant IT services to the healthcare industry comprising of healthcare institutions and healthcare service users.

Both healthcare service providers and healthcare service users benefit through availability and affordability of cloud services and a secured option, for the healthcare sector to deliver accessible and quality healthcare services. This is particularly crucial to the cost-sensitive private healthcare service providers like community hospitals, nursing homes, hospices and private clinics.

The scope of the project is to analyze and identify the gaps in the control requirements between MTCS standard and HITSecP, and recommend additional controls to cover such gaps. References are also made to the Advisory Guidelines for the Healthcare Sector issued by Personal Data Protection Commission (PDPC), Singapore (dated 11 September 2014), to ensure consistency and adequacy in covering such gaps.

2. NORMATIVE REFERENCES

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

- Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS584:2015)
- Healthcare IT Security Policy & Standards (HITSecP version 3.0, Oct 2014)

3. INFORMATIVE REFERENCES

The following source documents will be helpful to the audience in understanding this report:

- ISO/IEC 27001:2013 Information Security Management System – Requirements
- ISO/IEC 27002:2013 Information Security Management System – Code of Practice
- PDPC: Advisory Guidelines for the Healthcare Sector (11 September 2014)

4. PURPOSE OF DOCUMENT

This Gap Analysis Report is to assist CSPs that are MTCS certified to be able to comply with HITSecP and offer their services to private healthcare institutions.

Gap Analysis Report
The purpose of the gap analysis report is to provide an overview of the identified gaps of MTCS requirements against HITSecP. The information provided in this document aims to assist CSPs that are MTCS certified, to understand the specific expectations of HITSecP, as well as to assist healthcare institutions in assessing MTCS-certified CSP ability in meeting HITSecP expectations.

5. TARGET AUDIENCE

This Gap Analysis Report is meant for:

- CSPs who are MTCS-certified and wish to provide cloud services to healthcare institutions. CSPs will be able to understand the amount of effort and investments needed to meet HITSecP expectations.
- All healthcare institutions who wish to engage CSPs to provide cloud services. Through the use of this report, healthcare institutions will be able to conduct the necessary due diligence on CSPs who are certified to SS584.
- CBs who wish to provide certification services to MTCS-certified CSPs serving healthcare institutions against HITSecP.

6. DOCUMENT STRUCTURE

This document has the following structure from this section onwards. Sections 8, 9 and 12 have introduction statements that will explain the section's background and context in more details.

Section 7 – Terms and Definitions

Section 8 – Structural Understanding of Standards and Policies

Section 9 – Approach

Section 10 – Further Notes

Section 11 – Grading System

Section 12 – Summary of findings

Section 13 – Tips on using this Gap Analysis Report

Section 14 – Gap Analysis

Section 15 – Summary

Annex A

Annex B

7. TERMS AND DEFINITIONS

All terms used within this report are derived from HITSecP and SS584. Reader is advised to refer to the above-mentioned two documents in order to obtain the definitions if further clarity is needed. In case of conflicting terms and definitions provided within the two documents, SS584 terms and definitions will take precedence over HITSecP.

8. STRUCTURAL UNDERSTANDING OF POLICY & STANDARDS

It is necessary to understand the constraints when comparing standards against policies in general. Standards specify what is necessary to be implemented, in order to comply with the standards. Policies specify principles or declared objectives to guide decisions and achieve rational outcomes, intended results or a specific implementation expectation for the intended audience to adopt and conform. As specific implementation may be prescribed by the policy, it may be just one of the possible choices of implementation that the applied standard can accept. Hence, it is to say that having a CSP conforming to the standard, does not automatically mean that their implementation matches the expectations of the policy.

HITSecP is organized into three (3) hierarchical levels. The first level is known as chapter and this provides the topic of interest (from the perspective of ISO/IEC 27001 Annex A, this is known as security domain/context), the second level is known as section and this provides the description of the security area (from the perspective of ISO/IEC 27001 Annex A, this is known as security control) and the third level provides the governance statement of security area and/or the details of control.

SS584 is organized into three (3) hierarchical levels as explained below.

SS584 Hierarchical Levels	Explanation
Clause	Provides the topic of interest (from the perspective of ISO/IEC 27001, this is known as security domain/context/objective)
Sub-clause	Provides the sub-topic of interest
Standards requirements	Provides the requirements for conformance (from the perspective of ISO/IEC 27001 Annex A, this is known as security control) with 4 components namely general, Level 1 detailed requirements and audit procedures, Level 2 detailed requirements and audit procedures, and Level 3 detailed requirements and audit procedures (from the perspective of ISO/IEC 27002 and ISO/IEC 27008, this is known as implementation and audit guidance respectively).

The commonality between HITSecP and SS584, will be that the second level of both the policy and the standard as both documents are referring to security controls for implementation.

9. APPROACH

Prior to the comparison being done, the following assumptions have been made

1. Though HITSecP is applicable to all public healthcare institutions, this document that references public healthcare institutions, may also apply to CSPs who are providing cloud services to healthcare institutions.

2. Not all HITSecP statements are applicable to CSPs and hence, such statements are not subjected to gaps assessment. The applicability of HITSecP statements will be based on the following criteria:
   a. It is within the scope of cloud service outsourcing
   b. It is possible to be within CSP responsibility to manage the activity

3. The gaps assessment is applied against the CSPs who may be interested in providing cloud services to the healthcare institutions. These CSPs must be at least MTCS-certified, be it Level 1, 2 or 3. By default, CSPs who are certified to lower levels will require more effort and resources as compared to the CSPs that are certified to higher levels, in order to meet HITSecP.

4. During the assessment, if there are certain gaps that are only applicable to the implementation of certain cloud services, they will be highlighted so that when CSPs are seeking certification to HITSecP for the types of cloud services, they will be clear about the expectations.

5. As SS584 is technically a standard, it may be possible that MTCS provides additional requirements in fulfilling the controls. However, if the statements within HITSecP section do not mention about the need for these controls, such gaps will not be highlighted.

In order to enable CSPs (MTCS-certified) to serve healthcare institutions, requirements listed in the SS584 are matched with equivalent statements within the HITSecP. This follows a structured and systematic five (5) step approach:

1. For each of the HITSecP statements, identify the applicability of the statement based on the assumptions made.

2. For each applicable HITSecP section, identify the relevant SS584 clauses.

3. Review through all the statements within the HITSecP section and identify the sub-clauses within the SS584 clause which may have commonality.

4. The requirements identified in SS584 by level are then matched against the HITSecP statements to assess the area of commonality and its status. In the event where the HITSecP statement expectation is only met at higher level of MTCS controls (e.g. Level 3), the gap is likely to be identified for the lower levels of MTCS controls. If the HITSecP statement expectation is met at the lower levels of MTCS controls (e.g. Level 1), all higher levels of MTCS controls would also meet the HITSecP statement expectation as MTCS high levels build on lower levels.

5. For gaps which are immaterial, the reason, process and the criteria for the existence and alleviation of these gaps, would be re-looked into to ascertain whether any bridging is possible. The evaluation criterion has been further improved to incorporate the following: For findings which are technical based, the control principle will be derived and matched against the compared MTCS standard clause(s).

If there is a match, the partial gaps would be furnished with the remarks stating the control principles and minimum expectations required by the HITSecP, and be recommended to be considered as "included". WG also recommends that these gaps be re-verified.

6. The gaps identified in HITSecP statements are then consolidated at respective HITSecP sections for reporting purpose.

10. FURTHER NOTES

As SS584 is a requirement standard, it may be possible that MTCS provides additional requirements in fulfilling the controls mentioned in the HITSecP statement. However, if the statements within HITSecP section do not mention about the need for these specific controls, such differences will not be highlighted.

Furthermore, as HITSecP statements may have varying degrees of enforcements, only statements with "shall" or equivalent (e.g. must) will be evaluated. HITSecP statements with "should", equivalent or non-mandatory (e.g. may, can) will not be compared.

11. GRADING SYSTEM

The following are four (4) grading that are used within the gaps assessment.

Grading	Description
Included	indicates that HITSecP requirements are fully met by relevant MTCS clauses
Partial/Incremental	indicates that HITSecP section is stated with more details/requirements than the corresponding MTCS clauses or in situations where it is not affirmative that the MTCS fully fulfills the policy expectations
New	indicates that there are no matching MTCS clauses for the HITSecP requirements
Not Applicable	Indicates that the HITSecP statement is the responsibility of the healthcare organisation and CSP has no involvement in fulfilling /influencing it

In order to perform the gaps assessment, one must first understand both the SS584 requirements and HITSecP statements, in-depth.

HITSecP document has mainly three (3) statement writing styles

- The HITSecP statement contains only principles; the statement allows flexibility to the users of the HITSecP in terms of the expected implementations.
- The HITSecP statement contains detailed implementations; the statement is precise in terms of the implementation expectation for HITSecP users.
- The HITSecP statement refers to other related topics located in another chapter; the statement is trying to establish a link between two or more controls and is expecting to have the relationship to be explicit in terms of implementations.

There are three (3) possibilities where SS584 is matched against the HITSecP statements

- SS584 does not specify any requirements
- SS584 specifies principles of implementation requirement
- SS584 specifies detailed implementation requirements

HITSecP statement contains …	Principles	… Contains detailed implementation	Bridging security topics *(e.g. with control A, one can implement control B)*
MTCS does not specify any requirements	***New***	***New***	***New***
MTCS specifies principles of implementation requirement	***Included,*** if the HITSecP statement can be fulfilled by MTCS implementation principles ***Partial***, if the HITSecP statement contains more implementation principles than MTCS has specified	***Partial***, if HITSecP statement matches with the intent of the MTCS implementation principles	***Included***, if intent of the HITSecP statement matches MTCS implementation principles ***Partial,*** if the intent of HITSecP statement has more coverage than MTCS implementation principles
MTCS specifies detailed implementation requirement	***Included,*** if the HITSecP statement can be fulfilled by MTCS implementation requirement ***Partial,*** if MTCS implementation requirement does not completely fulfil the HITSecP statement	***Included***, if the HITSecP statement can be fulfilled by MTCS implementation requirement ***Partial,*** if HITSecP statement cannot be completely fulfilled with MTCS implementation requirement	***Included***, if the intent of the HITSecP statement can be fulfilled by the MTCS implementation requirement ***Partial***, if the intent of HITSecP statement cannot be completely fulfilled by MTCS implementation requirement

12. SUMMARY OF FINDINGS

It is important to note that the target beneficiaries are healthcare institutions. Based on the existing operating healthcare applications-related environment and expectations, only MTCS certification at Level 3 is relevant for comparison.

The table below provides a high level summary of the differences between HITSecP and MTCS Level 3. CSPs that are **MTCS Level 3** certified and wish to comply with HITSecP, can refer to this table for gaps applicable to this level.

Total Policy Statements in HITSecP	Not Applicable		Included		Incremental		New	
	Total	%	Total	%	Total	%	Total	%
256	112	43.75	128*	50	16	6..25	0	0

The table shows that there are total of **256 statements in HITSecP** which were compared against MTCS. The breakdown is as follows:

- HITSecP statements that specify the responsibility of the healthcare organisations and CSP has no involvement in fulfilling /influencing them, are termed **(Not Applicable) = 112**;

- HITSecP statements that are fully met by relevant MTCS clauses, are termed **(Included) = 128**. Amongst the 128, 12 statements need further verification and can be found in Annex B with the phrase duly attached "Included (needs further verification)";

- HITSecP statements which have more details/requirements than the corresponding MTCS clauses or in situation where it is not affirmative that the MTCS fulfils the policy expectations, are termed **(Partial /Incremental)** gaps **= 16**;

- No matching MTCS clauses for the HITSecP requirements are termed **(New) = 0.**

13. TIPS ON USING THIS GAP ANALYSIS REPORT

The description of the respective columns in the gap analysis table in Section 14 'Gap Analysis' is listed below:

1. The column "Policy Statement" specifies the statement reference number of the HITSecP.

2. The column “Reference to matching MTCS sub-clauses” specifies the sub-clauses that are currently stated in the MTCS, and have equal requirements or components relevant to the corresponding HITSecP statement under the column “Policy Statement”.
3. The column “Remarks on identified gaps” denotes observations and additional notes based on the gap analysis.

14. GAP ANALYSIS

The purpose of this section is to identify the gaps of MTCS requirements against HITSecP. The table below summarises the list of statements in HITSecP and the respective classification of gaps in relation to MTCS Levels 3 requirements. Even though there are only 16 partial gaps in this section, there are 12 items in Annex B that need to be re-verified:

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
1	14.1.16	While ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that specialist advice should be obtained on how to avoid damage from fire. Additional information on the need for emergency exits and requirements could be found in SCDF Fire Code 2013 Chapter 2.11 Means of Escape. There is no information provided on testing requirements. The rationale behind the need for emergency exits and the testing requirements to ensure these exists are used only during emergencies should have been considered during risk assessment and subsequently the implementation phase.	18 Physical and environmental	18.5 Environmental threats and equipment power failure	A.11.1.4	N.A

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
2	14.4.3	ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that specialist advice should be obtained on how to avoid damage from fire. SCDF Fire Code 2013 Chapter 2.11 Means of Escape suggests some details about a fire escape route/plan, portable fire extinguishers etc. The rationale behind the need for fire safety and emergency procedures to protect human lives should have been considered and addressed for implementation.	-	-	A.11.1.4	More advice pertaining to this control should be sought from local fire safety regulations or building codes.
3	14.4.4	ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that specialist advice should be obtained on how to avoid damage from fire. The rationale behind having centrally-managed visual and audible alarm notification system to alert personnel during emergencies, should have been considered during risk assessment and implemented.	18 Physical and environmental	18.5 Environmental threats and equipment power failure	A.11.1.4	More advice pertaining to this control should be sought from local fire safety regulations or building codes.
4	14.4.5	ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that	18 Physical and environmental	18.5 Environmental threats and	A.11.1.4	More advice pertaining to this control should be sought from local

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		specialist advice should be obtained on how to avoid damage from fire. MTCS Clause 18.5.2(d) mentions that a fire protection and suppression system with, but not limited to, peripherals such as handheld fire extinguishers and smoke detectors must be installed. Therefore since the MTCS clause gives room for additional components such as audible alarm, to be installed as necessary. The rationale behind having a fire protection and suppression system, should have been considered during risk assessment and implemented.		equipment power failure		fire safety regulations or building codes.
5	14.4.6	ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that specialist advice should be obtained on how to avoid damage from fire. MTCS Clause 18.5.2(d) mentions the use of fire protection systems having portable fire extinguishers, while no reference is made to	18 Physical and environmental	18.5 Environmental threats and equipment power failure	A.11.1.4	The control is to prevent loss of lives and reduce /limit damage to property More advice pertaining to this control should be sought from local fire safety regulations or building codes.

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		them being installed throughout the site. SCDF Fire Code 2013 Chapter 6.1 also mentions about the usage and installation of portable fire extinguishers. The rationale behind the installation and usage of portable fire extinguishers should have been considered during risk assessment and implemented.				
6	14.4.7	ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that specialist advice should be obtained on how to avoid damage from fire. MTCS Clause 18.5.2(a) mentions that any adequate physical and environmental fire protection measures for office, rooms and information processing facilities need to be installed. This seem to suggest that any viable or stronger alternatives, which also are able to contain the fire and prevent loss of life and limit damage to property could be installed.	18 Physical and environmental	18.5 Environmental threats and equipment power failure	A.11.1.4	The control is to contain the fire, prevent loss of lives and reduce /limit damage to property. MTCS Clause 18.5.2 (a) mentions that fire-rated walls, surrounding computer facilities should be non-combustible and resistant to fire for at least one-hour. Mention is also made for any openings to these walls (doors, ventilation, and ducts) should be self-closing and fire-rated for an hour. MTCS seems to suggest that any viable or even stronger alternatives, meeting the original principles of containment, protection of lives and property could be implemented.

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		The rationale behind the conditions that fire-rated walls, doors, ventilations and ducts etc. should have been considered during risk assessment and implemented.				More advice pertaining to this control should be sought from local fire safety regulations or building codes.
7	14.4.8	ISO/IEC 27002:2013 ISMS COP, Clause 11.1.4 mentions that specialist advice should be obtained on how to avoid damage from fire. While the there is no mention of monitoring , bi-yearly testing and documentation of test results for fire suppression equipment in MTCS Clause 18.5.2(d), there is mention of the system being maintained regularly to thwart unexpected fire. This could suggest that an equivalent or even stronger maintenance plan could be put in place to adhere to the principles of having a well-maintained and operational fire suppression system. The rationale behind monitoring, testing and documentation of test results for fire suppression equipment should have been	18 Physical and environmental	18.5 Environmental threats and equipment power failure	A.11.1.4	Principle behind this control is for the fire suppression equipment to be well-maintained and operational at all times. MTCS Clause 18.5.2 (d) mentions about fire protection systems and suppression systems being installed and maintained regularly to thwart unexpected fire. The terms “maintained” and “thwart unexpected fires” seem to suggest that the system must be serviced and tested regularly to be operable at any instant. More advice pertaining to this control should be sought from local fire safety regulations or building codes.

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		considered during risk assessment and implemented.				
8	14.4.9	While MTCS Clause 18.5.2(d) mentions that fire protection and suppression systems shall be installed and maintained regularly, including portable fire extinguishers, there is no explicit mention of computer room personnel being trained. The rationale behind training computer room personnel on the use of automatic suppression systems, portable fire extinguishers and response to smoke and fire alarms, should have been considered during risk assessment and implemented.	18 Physical and environmental	18.5 Environmental threats and equipment power failure	-	More advice pertaining to this control should be sought from local fire safety regulations or building codes.
9	14.4.10	ISO/IEC 27002 ISMS COP Clause 11.1.4 mentions that specialist advice should be sought to avoid damage from fire. SCDF Fire Code 2013 Chapter 2.1.1 Means of escape, which talks about a fire escape plan and its implementation and, may serve as a reference. The rationale behind having visual procedures and fire drills to	-	-	A.11.1.4	More advice pertaining to this control should be sought from local fire safety regulations or building codes.

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		ensure safe evacuation of personnel during emergency should have been considered during risk assessment and implemented				
10	14.5.3	While the requirement mentions about periodic inspection, testing and maintenance for all systems, MTCS Clause 18.5.2(c) mentions detecting any anomalies in the temperature and humidity environmental control system and taking any immediate action. This seems to suggest that inspection maintenance and testing may be undertaken when necessary. The rationale behind periodic inspection, maintenance and testing for all systems should have been considered during risk assessment and implemented.	18 Physical and environmental	18.5 Environmental threats and equipment power failure	-	The requirement is to ensure that all the systems in the facility are well-maintained and operational at all times. MTCS Clause 18.5.2 (c) indicates detecting any anomalies in the temperature and humidity environmental control system and taking any immediate action. While there is no mention of periodic inspection and testing of the systems, the MTCS clause seems to suggest that inspection, maintenance and testing may be undertaken when necessary.
11	16.2.4	While the requirement mentions that emergency-use service IDs that are used for remote problem solving or fault resolution, shall be enabled only upon requirement and disabled when completed, ISO/IEC 27002 ISMS COP Clause A.11.2.8 stipulates that active sessions should be terminated when finished unless	22 Cloud Services Administration	22.1 Privilege account creation	A.11.2.8	N.A

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		secured by an appropriate locking mechanism or logged-off from applications or network services when no longer needed. There is no clear mention whether this pertains to service-IDs or relates to third-party access in this case. For example, are contractors adhering to this policy, if they remote access to perform checks on the system. The need for enablement, termination of remote access service and disablement of service-ID after use, should have been considered during risk assessment and implementation.				
12	16.3.5	While the requirement mentions about periodic review with regards to dormant and unused accounts and the disablement of the unused accounts to prevent unauthorized access, ISO/IEC 27002 ISMS COP Clause A.9.2.5 (a & d) is general and stipulates that user rights and privileged allocations should be reviewed at regular intervals, after any changes in employment and for unauthorized privileges.	22 Cloud Services Administration	22.3 Administer access review and revocation	A.9.1.1 (h) A.9.2.5(a & d)	N.A

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		Additionally, usage trends need to be also reviewed while checking for dormant and unused accounts. The management of unused or dormant accounts, similar to administers, should have been considered during risk assessment and implemented.				
13	16.4.7	MTCS Clause 22.42(a) says account shall be locked out after a maximum of 6 unsuccessful attempts but the policy mentions 5 unsuccessful attempts only.	22 Cloud Services Administration	22.4 Account lockout	-	N.A
14	16.8.1	ISO/IEC 27002: 2013 ISMS COP Clause 12.1.4 (c) mentions that compilers and system utilities should not be accessible from operational systems, when not required. By default, compilers should not be accessible for operational systems and hence, installation would have been discouraged, however, on the event where it is installed, the restriction is unclear. Examples include the java complier which is required online and machines like mainframes which are too expensive to have	14 Secure Configuration	14.5 Restriction to System Utilities	A.12.1.4	N.A

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		another server just for separate development. Organisation should have identified and implemented the control for restricting access to operational software.				
15	17.3.5	According to ISO/IEC 27002 ISMS COP Clause 12.6.2, the organisation should identify the type of software installations permitted, prohibited and those with a malicious pedigree. MTCS Clause 14.8 mentions that mechanisms should be implemented to prevent unauthorized software. While the term unauthorized suggests that the software is not permitted, unlicensed seems to indicate some illegality about the software, which also should not be permitted due to legal issues that could occur. Therefore, both terms may or may not be interchanged and hence, detection and prevention of unauthorized and unlicensed software installation should have	14 Secure configuration	14.8 Unauthorised Software	A.12.6.2	N.A

S/N	Policy Statement	L3 Gaps	Reference to matching MTCS Clauses	Reference to MTCS sub-clauses	ISO/IEC 27001:2013 ISMS	Remarks on identified gaps
		been considered during risk assessment and implemented.				
16	17.6.2	Although MTCS Clause 17.1 mentions that requirements for key rotation must be considered in the policies and procedures, no mention is made about the key change intervals stated in the requirements.	17 Encryption	17.1 Encryption policies and procedures	A.10.1.2	Cryptographic keys may be changed routinely or ad-hoc and MTCS does not address changing of keys routinely but, the principle of changing of keys remain.

15. SUMMARY

This Gap Analysis Report assists CSPs that are MTCS-certified, to align themselves with HITSecP so as to be able to serve the healthcare institutions.

The gap analysis involves matching the existing MTCS requirements against HITSecP policies. The information provided in this document aims to assist CSPs that are MTCS-certified, to understand the specific expectations of HITSecP as well as to assist healthcare institutions in assessing CSP ability in meeting HITSecP expectations. While there are Incremental Gaps (refer to Sections 12, 14 and Annex B for details), they are considered minor and inconsequential.

The WG has completed their study of MTCS's 3-tier levels and established that a mapping table that provides guidance on the types of healthcare information/data that may be hosted on the different MTCS levels.

Under the MTCS model, Level 3 certification would be suitable for clinical and patient administrative support systems that process and store patient electronic medical and healthcare records. MTCS Level 2 certification would be appropriate for IT enterprise support and administration systems that process and store operational data while MTCS Level 1 certification is suitable for hosting non-sensitive public information.

MTCS Levels	Application/ System Types*	Data
L3	Clinical and patient administrative support systems	Patient electronic medical and health records, including diagnosis, medication prescriptions, billing and admissions, patient-generated health information.
L2	IT enterprise support and administration systems	Operational data including employee information, medication inventory and purchase management.
L1	Public Information Systems	Publicly available information including informational websites, clinical standards and terminology systems, medical practitioners registries.

**MTCS certification can be obtained at the infrastructure level (Infrastructure as a Service (IAAS) or Platform as a Service(PAAS)) or at an application level, i.e. Software as an Application (SAAS) level. Healthcare providers hosting their IT applications with MTCS-certified infrastructure providers will need to carry out their due diligence and implement appropriate additional security and controls for their applications in line with their risk assessment and security policies*

ANNEX A

The following is a table of excluded HITSecP requirements and the reasons for exclusion.

S/N	Policy Statement	Reason for exclusion
1	1.1.1	This is an introduction on the importance of having information security for the healthcare institution.
2	1.1.2	This is an introduction on the importance of having information security for the healthcare institution.
3	1.1.3	This is an introduction on the importance of having information security for the healthcare institution.
4	2.1.1	This is to set the need for IT security policies and standards adoption by the healthcare institution.
5	2.1.2	This is to set the need for IT security policies and standards adoption by the healthcare institution.
6	3.1.1	This mentions the source of reference.
7	3.1.2	This mentions the source of reference.
8	3.1.3	This mentions the source of reference.
9	4.1.1	This mentions the principles of IT security to be adopted by the healthcare institution.
10	4.2.1	This mentions the principles of IT security to be adopted by the healthcare institution.
11	4.3.1	This mentions the review period of the HITSECP, which the healthcare institution will need to take care of.
12	4.3.2	This mentions the review period of the HITSECP, which the healthcare institution will need to take care of.
13	4.3.3	This mentions the review period of the HITSECP, which the healthcare institution will need to take care of.
14	4.3.4	This mentions the review period of the HITSECP which, the healthcare institution will need to take care of.
15	5.1.1	This IT governance framework is to be established within each healthcare institution.
16	5.2.1	This IT governance framework is to be established within each healthcare institution.
17	5.2.2	This IT governance framework is to be established within each healthcare institution.
18	5.2.3	This IT governance framework is to be established within each healthcare institution.
19	5.2.4	This IT governance framework is to be established within each healthcare institution.
20	5.2.5	This IT governance framework is to be established within each healthcare institution.
21	5.2.6	This IT governance framework is to be established within each healthcare institution.
22	6.1.1	This is not applicable since this is the healthcare institution’s roles and responsibilities to CSP; they are only the receiving end.
23	6.2.1	This is not applicable since this is the healthcare institution’s roles and responsibilities to CSP; they are only the receiving end.

S/N	Policy Statement	Reason for exclusion
24	6.2.2	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
25	6.2.3	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
26	6.2.4	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
27	6.3.1	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
28	6.4.1	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
29	6.5.1	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
30	6.6.1	This is not applicable since this is the healthcare institution's roles and responsibilities to CSP; they are only the receiving end.
31	7.1.2	This is the healthcare institution's responsibility to maintain an IT systems inventory.
32	7.1.5	This is the healthcare institution responsibility to ensure that risk assessment, vulnerability management and disaster recovery planning are initiated through the inventory listing.
33	8.1.2	This is the healthcare institution's responsibility as any deviation can only be raised by the institution themselves.
34	8.1.3	This is the healthcare institution's responsibility as any deviation can only be raised by the institution themselves.
35	8.1.4	This is the healthcare institution's responsibility as any deviation can only be raised by the institution themselves.
36	8.1.5	This is the healthcare institution's responsibility as any deviation can only be raised by the institution themselves.
37	8.1.6	This is the healthcare institution's responsibility as any deviation can only be raised by the institution themselves.
38	8.1.7	This is the healthcare institution's responsibility as any deviation can only be raised by the institution themselves.
39	9.1.1	This activity must be initiated by the healthcare institution as they need to perform at least the final review of the compliance report.
40	9.1.2	This activity must be initiated by the healthcare institution as they need to perform at least the final review of the compliance report.
41	9.1.3	This activity must be initiated by the healthcare institution as they need to perform at least the final review of the compliance report.
42	10.1.1	This activity must be initiated from the healthcare institution.
43	10.1.2	This activity must be initiated from the healthcare institution.

S/N	Policy Statement	Reason for exclusion
44	12.1.1	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
45	12.1.2	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
46	12.2.1	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
47	12.2.2	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
48	12.2.3	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
49	12.3.1	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
50	12.4.1	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
51	12.4.2	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
52	12.5.1	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
53	12.5.2	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
54	12.5.3	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
55	12.5.4	Information classification cannot be outsourced as it is the responsibility of the healthcare institution.
56	12.6.1	The methods of access control should be defined by the healthcare institution and not the CSP.
57	12.6.2	The methods of access control should be defined by the healthcare institution and not the CSP.
58	12.6.3	The methods of access control should be defined by the healthcare institution and not the CSP.
59	12.7.1	CSP cannot influence the transmission methods of confidential information as it is only at the receiving end.
60	12.8.1	CSP cannot influence the transmission methods of confidential information as it is only at the receiving end.
61	12.8.2	CSP cannot influence the destruction methods of confidential information, it is only at the receiving end.
62	13.1.1	This control needs to be initiated from the healthcare institution, not the CSP.
63	13.1.2	This control needs to be initiated from the healthcare institution, not the CSP.
64	13.1.3	This control needs to be initiated from the healthcare institution, not the CSP.
65	13.2.1	This control needs to be initiated from the healthcare institution, not the CSP.
66	13.3.2	This is initiated from the healthcare institutions and not from the CSP.
67	13.3.3	This is initiated from the healthcare institutions and not from the CSP.
68	13.4.1	CSP does not have any involvement in this area.
69	13.4.2	CSP does not have any involvement in this area.
70	15.1.1	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
71	15.1.2	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.

S/N	Policy Statement	Reason for exclusion
72	15.1.3	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
73	15.1.4	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
74	15.1.5	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
75	15.1.6	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
76	15.1.7	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
77	15.1.8	The outsourcing decision is to be made by the healthcare institution and not the CSP even though the CSP may further outsource its services and will be covered under MTCS.
78	15.2.6	This is the liability of the healthcare institutions to ensure confidential information, including personal data, is not used for development or testing purposes, unless anonymised or masked.
79	15.3.2	If segregation of duties is not feasible or practical, it is the healthcare institution’s responsibility to look for another CSP.
80	15.5.1	CSP has no involvement in wireless service deployment.
81	15.5.2	CSP has no involvement in wireless service deployment.
82	15.5.3	CSP has no involvement in wireless service deployment.
83	15.5.4	CSP has no involvement in wireless service deployment.
84	15.9.1	CSP has no involvement in endpoint device deployment.
85	15.9.2	CSP has no involvement in endpoint device deployment.
86	15.9.3	CSP has no involvement in endpoint device deployment.
87	15.9.4	CSP has no involvement in endpoint device deployment.
88	15.9.5	CSP has no involvement in endpoint device deployment.
89	15.9.6	CSP has no involvement in endpoint device deployment.
90	15.9.7	CSP has no involvement in endpoint device deployment.
91	15.10.1	CSP has no involvement in managing removable storage media.
92	15.10.2	CSP has no involvement in managing removable storage media.
93	15.10.3	CSP has no involvement in managing removable storage media.
94	15.10.4	CSP has no involvement in managing removable storage media.

S/N	Policy Statement	Reason for exclusion
95	15.10.5	CSP has no involvement in managing removable storage media.
96	15.10.6	CSP has no involvement in managing removable storage media.
97	15.10.7	CSP has no involvement in managing removable storage media.
98	15.12.1	Accessibility and network connectivity shall be managed by the healthcare institution.
99	15.12.2	Accessibility and network connectivity shall be managed by the healthcare institution.
100	15.12.3	Accessibility and network connectivity shall be managed by the healthcare institution.
101	15.12.4	Accessibility and network connectivity shall be managed by the healthcare institution.
102	16.1.1	This is the healthcare institution's responsibility as the organisation will need to define the access control within the institution.
103	16.1.2	This is the healthcare institution's responsibility as the organisation will need to define the access control within the institution.
104	16.1.3	This is the healthcare institution's responsibility as the organisation will need to define the access control within the institution.
105	16.1.4	This is the healthcare institution's responsibility as the organisation will need to define the access control within the institution.
106	16.3.2	CSP will not be able to detect this issuance of multiple accounts to the same user.
107	16.5.1	The provisioning of teleworking facilities is the responsibility of the healthcare institution, it cannot be outsourced.
108	17.3.6	CSP has no involvement in endpoint device deployment.
109	17.5.3	CSP has no involvement in endpoint device deployment.
110	17.5.4	CSP has no involvement in endpoint device deployment.
111	18.2.1	This will be the healthcare institution responsibilities to seek for professional advisory as well as information for the senior executives of the organisation.
112	18.2.5	This will be the healthcare institution responsibilities to ensure reporting conforms to MOHH/IHiS IT Security Incident Response Framework (ITSIRF) and MOHH/IHiS IT Security Incident Response Plan and Procedure.

ANNEX B

The following table shows the HITSecP policy statements which are applicable but fully met by MTCS L3 controls. Please do note that there are 12 items in this section that need further verification. These can be identified by the phrase "Included (needs further verification)".

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
1	7.1.1	19.4	Contractual agreements or other means of acceptable communication acceptable to the cloud users, should contain the service levels and performance (including subsequent changes) defined by the CSP.	Included	N.A
2	7.1.3	18.1	For IaaS and PaaS environment, there is no mention in the standard that requires periodic reviews against the healthcare institutions assets. Since this is an extension of security protection stated in MTCS Clause 18.1, it could be considered as included.	Included (needs further verification)	The principle behind this control is to ensure that the inventory is regularly verified for its currency. The word maintain also seems to suggest that the inventory is regularly reviewed to include new details such as changing of ownership or location. This needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
3	8.1.1	6.1	Organisation should have identified and implemented the control for the source of non-compliance identification against HITSecP, where CSP will need to focus on non-compliance identification, since it is explicitly identified in ISO/IEC 27002 ISMS COP Clause 18.2.2(a): identify the causes of non-compliance, for consideration.	Included	The expectation of this control is to ensure that the outcome of review and audit processes need to be followed up. The auditor will need to verify that the controls implemented by CSP would have the minimum 4 sources of input.
4	11.1.1	8.1	A cloud-specific risk management programme should be established and maintained by CSP.	Included	N.A
5	11.2.1	8.1	A cloud-specific risk management programme should be established and maintained by CSP.	Included	N.A
6	11.2.2	8.1	A cloud-specific risk management programme should be established and maintained by CSP.	Included	N.A
7	11.3.1	8.1	A cloud-specific risk management programme should be established and maintained by CSP.	Included	N.A
8	11.3.2	8.1	A cloud-specific risk management programme should be established and maintained by CSP.	Included	N.A
9	12.9.1	11.3	Information security Incident Reporting Process shall be established by CSP.	Included	N.A
10	13.3.1	23.2	Requirements and audit procedures pertaining to user	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			access to the cloud environment, should be established by CSP.		
11	14.1.1	18.3	Procedures to ensure physical security and safety of cloud information processing facilities, should be established by CSP.	Included	N.A
12	14.1.2	18.3	According to 11.1.3 (b) of ISO/IEC 27002 ISMS COP, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities.	Included	Organisation should have identified and implemented the control for restricting directional signage since it is explicitly identified in ISO/IEC 27002 ISMS COP for consideration.
13	14.1.3	18.3	Procedures to ensure physical security and safety of cloud information processing facilities, should be established by CSP.	Included	N.A
14	14.1.4	18.3	The requirement specifically mentioned on the need to implement card key and access code systems, combination pin lock systems, automatic door - closer and CCTV camera and recording systems, or equivalent as the means for physical protection while MTCS Clauses 18.32 (d) and (b) did have more general expressions of physical access protection –physical access to information systems and assets	Included (needs further verification)	The rationale of this control is to prevent unauthorized access into restricted information processing areas using technology such as CCTV. This needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			shall be restricted and surveillance systems shall monitor access to and within the data centre. As such, it could be considered as included.		
15	14.1.5	18.3	Procedures to ensure physical security and safety of cloud information processing facilities, should be established by CSP.	Included	N.A
16	14.1.6	18.3	ISO/IEC 27002 ISMS COP Clause 11.1.2(b) mentions that all external doors should be suitably protected against unauthorized access with control mechanisms and doors and windows should be locked when unattended. ISO/IEC 27002 ISMS COP Clause 11.1.2(c) mentions that access to site and buildings should be restricted to authorized personnel only. This seems to suggest that either locking mechanisms or the equivalent should be used to restrict access to the rooms, to authorized personnel only. Organisation should have identified and implemented the control for locking doors at all	Included	Locking doors at all times and having authorised personnel having the combination or key are basic controls of physical protection. Alternate implementation would be acceptable as long as these controls are of the same strength or better.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			times, with only authorised personnel having the combination or key, since it is explicitly identified in ISO/IEC 27002 ISMS COP for consideration.		
17	14.1.7	18.3	ISO /IEC 27002:2013 ISMS COP Clause 11.2.3 (c) mentioned that controlled access to cable rooms should be considered for sensitive and critical systems. This seems to suggest that either locking mechanisms or the equivalent should be used to restrict access to the rooms, to authorized personnel only. MTCS Clause 18.3.2(a) mentions that physical access to communications hardware should be restricted. It could be assumed that communication hardware and communication wiring rooms need to be secured together as they cannot function separately. The rationale behind locking rooms containing wiring and communications equipment and restricted access to personnel, should have been considered during risk assessment and	Included (needs further verification)	The principle behind this control is reduce the opportunity of eavesdropping through wiretapping. Though MTCS Clause 18.3.2(a) mentions that physical access to communications hardware should be restricted. It could be assumed that communication hardware and communication wiring rooms need to be secured together as they cannot function separately. This needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			implemented. As such, this could be changed to included.		
18	14.1.8	18.4	User access to the Cloud Information Processing Facilities, should be restricted by the CSP.	Included	N.A
19	14.1.9	-	According to Clause 11.1.2 (d) of ISO/IEC 27002:2013 ISMS COP, employees' contractors and external parties should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. The rationale behind nabbing unauthorised personnel and calling for additional assistance and advisory should have been considered during risk assessment and implemented. As this is explicitly mentioned in ISO/IEC 27002:2013 ISMS COP Clause 11.1.2 (d), this could be changed to included.	Included (needs further verification)	Need further verification.
20	14.1.10	18.4	User access to the Cloud Information Processing Facilities, should be restricted by the CSP.	Included	N.A
21	14.1.11	22.10	Duties and areas of responsibilities should be segregated by the CSP, to reduce unauthorized or	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			unintentional modification or misuse of information assets.		
22	14.1.12	-	According to ISO/IEC 27002: 2013 ISMS COP Clause 11.1.2(b),(f) access to areas where confidential information is processed or stored should be restricted to authorized individuals only and access rights to secure areas should be regularly reviewed and updated. Organisation should have identified and implemented the control for having an up-to-date list of personnel who possess the cards/keys to computing facilities, and ensure that they are maintained, since it is explicitly identified.	Included	N.A
23	14.1.13	11.3	Although there is an information security incident reporting process requirement, there is no explicit mention about the handling of loss-of-access cards/key to computing facilities in MTCS Clause 11.3. It is expected of the organisation to take into consideration of loss-of-access cards/key situation; it is assumed that it will be part of the information security incident	Included (needs further verification)	The principle behind this control is to minimise the window of possible compromise due to loss of access cards/keys. MTCS Clause 11.3.2(a) mentions about the appropriate management must be informed for any incidents according to pre-defined communication. Therefore, this also needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			response handling process and is considered as included.		
24	14.1.14	-	According to ISO/IEC 27002: 2013 ISMS COP Clause 11.1.5(a), personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis. Organisation should have identified and implemented the control for the need for instructions on appropriate behaviour while working at the computing facilities, since it is explicitly identified in ISO/IEC 27002 ISMS COP for consideration.	Included	N.A
25	14.1.15	18.3 ~ 18.4	Physical security and safety of the cloud information processing facilities, shall be ensured by the CSP. Visitor access to the cloud information processing facilities, shall be restricted by CSP.	Included	N.A
26	14.2.1	18.2	Requirements and audit procedures pertaining to off-site movement, shall be implemented by CSP.	Included	N.A
27	14.2.2	18.1	ISO/IEC 27002 ISMS COP Clause 11.2.5(c) mentions that assets to	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			be recorded when removed off-site and returned. Organisation should have identified and implemented the control for tracking the equipment movement, since it is explicitly identified in ISO/IEC 27002 ISMS COP for consideration.		
28	14.3.1	18.3,18.5	Physical security and safety of the cloud information processing facilities, shall be ensured by the CSP. Guidelines for cloud infrastructure, equipment, power and telecommunication cabling, that should be communicated to all personnel working in the cloud information processing facilities, should be established by the CSP.	Included	N.A
29	14.3.2	18.3	Though the requirement mentions that server racks need to be locked and keys made accessible only to authorized personnel, MTCS Clause 18.3.2(d) details about the need for physical access to information systems and assets, to be restricted. This seems to indicate that either a lock and key mechanism or any	Included (needs further verification)	The rationale behind the control is prevent unauthorized access to server racks or equipment. MTCS Clause 18.3.2(d) mentions that all physical access to information systems and assets shall be restricted. This does suggest that any physical access restricting controls, even those alternatives of the same strength or stronger than a lock

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			other possible alternatives addressing the same concern could be implemented. Hence, it could be considered as included.		and key system, could be employed. This needs further verification.
30	14.3.3	18.4	Visitor access to the cloud information processing facilities, shall be restricted by CSP.	Included	N.A
31	14.3.4	18.5	Guidelines for cloud infrastructure, equipment, power and telecommunication cabling, that should be communicated to all personnel working in the cloud information processing facilities, shall be established by the CSP.	Included	The physical protection is unclear. It is assumed that there is protection of power and telecommunications equipment and cabling - including protecting control boxes, cables, wiring hubs and other equipment from fire vandalism, and interception of communications or disruption of service.
32	14.3.5	21.2	BCP and DR plans shall be implemented and developed by CSP.	Included	N.A
33	14.4.1	18.5	Guidelines for cloud infrastructure, equipment, power and telecommunication cabling, that should be communicated to all personnel working in the cloud information processing facilities, shall be established by the CSP.	Included	Though there is mention about the need for smoke detectors and held fire extinguishers, the need for dry pipe water sprinkler systems is not mentioned in the requirement.
34	14.4.2	18.5	Guidelines for cloud infrastructure, equipment, power and telecommunication cabling, that	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			should be communicated to all personnel working in the cloud information processing facilities, shall be established by CSP.		
35	14.5.1	18.5	Guidelines for cloud infrastructure, equipment, power and telecommunication cabling, that should be communicated to all personnel working in the cloud information processing facilities, shall be established by CSP.	Included	Air-conditioning is considered to be a given, since temperature is monitored. The requirement is not explicit about having alarms installed for temperature and humidity monitors. Also same goes for UPS, battery and backup power supply.
36	14.5.2	18.5	Guidelines for cloud infrastructure, equipment, power and telecommunication cabling, that should be communicated to all personnel working in the cloud information processing facilities, shall be established by CSP.	Included	N.A
37	14.5.4	-	While the requirement says that operational site personnel should be trained to monitor and control various devices (environmental control), ISO/IEC 27002 :2013 ISMS COP Clause 7.2.1(f) mentions that staff need to have appropriate skills and qualifications and need to be educated on a regular basis. Organisation should have identified and implemented the	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			control for the need to train operational site personnel to monitor and control the various equipment and devices.		
38	15.2.1	20.1	Change management process for its production information processing facilities and systems, shall be implemented and maintained by CSP.	Included	N.A
39	15.2.2	20.1	Change management process for its production information processing facilities and systems, shall be implemented and maintained by CSP.	Included	N.A
40	15.2.3	20.1	Change management process for its production information processing facilities and systems, shall be implemented and maintained by CSP.	Included	N.A
41	15.2.4	20.2	Backup procedures for changes, shall be implemented and maintained by CSP.	Included	N.A
42	15.2.5	20.1	Change management process for its production information processing facilities and systems, shall be implemented and maintained by CSP.	Included	Though this is not explicit but for MTCS-certified CSP, the need to maintain records is a given.
43	15.3.1	22.10	Duties and areas of responsibilities should be segregated by CSP, to reduce unauthorized or	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			unintentional modification or misuse of information assets.		
44	15.4.1	24.3	A secure network architecture should be implemented and managed by CSP, to protect the cloud infrastructure (systems, applications and data).	Included	N.A
45	15.4.2	24.3	A secure network architecture should be implemented and managed by CSP, to protect the cloud infrastructure (systems, applications and data).	Included	N.A
46	15.4.3	11.1, 13.1, 15.3	An information security incident response plan and procedures to respond to incidents in a timely fashion, should be implemented and maintained by CSP. Process of tracking and monitoring of all access to the network resources and system components, shall be established by CSP. A security monitoring process shall be in put in place by CSP.	Included	N.A
47	15.4.4	24.3	A secure network architecture should be implemented and managed by CSP, to protect the cloud infrastructure (systems, applications and data).	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
48	15.4.5	18.4	Restriction of visitor access to cloud information processing facilities, should be implemented by CSP.	Included	N.A
49	15.4.6	22.7	Administration of cloud infrastructure is protected from unauthorized changes, by CSP.	Included	N.A
50	15.6.1	13.1, 13.3	Process of tracking and monitoring of all access to the network resources and system components, shall be established by CSP. Audit trails of access to network resources and system components are captured and protected by CSP.	Included	N.A
51	15.6.2	23.6	While the requirement states that passwords should not be stored in clear text (hashed), MTCS Clause 23.62(c) mentions that password storage needs to be encrypted. Since both of these are working on the principles of password safekeeping in logs and audit trails, even an equivalent or stronger alternative such as a strong encryption key could be implemented. Hence, it could be considered as included.	Included (needs further verification)	The control is to prevent passwords from being retrieved directly from logs/audit trails and being used to compromise systems. MTCS Clause 23.6.2 c mentions about protecting passwords by encrypting the storage. An equivalent or stronger form of encryption could be used to store the passwords and protect the system, which adheres to the same principles. This needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
52	15.6.3	13.2	Process for log review shall be undertaken by CSP.	Included	N.A
53	15.6.4	13.2	Process for log review shall be undertaken by CSP.	Included	The policy uses "may"; leaving the ability to implement using suitable methods.
54	15.6.5	13.1,13.4	Process of tracking and monitoring of all access to the network resources and system components, shall be established by CSP. Log retention procedure shall be established by CSP.	Included	N.A
55	15.6.6	13.2	Process for Log review shall be undertaken by CSP.	Included	It is assumed that systems and services performing security functions equate to infrastructure components described in the policy.
56	15.6.7	13.2	MTCS Clause 13.2.3 (a) states that log review for all system components daily including those of critical systems and servers performing security functions (E.g. intrusion detection system and authentication servers), must be done daily. Even though, the scope of implementation is not defined, it is assumed that the event logs will be monitored for increase in traffic or unusual surges/patterns, increase in the number of dropped packets	Included	NA

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			in firewall logs, high volume of traffic to web servers from same IP addresses, unusual surge in CPU utilisation on web, application or proxy servers and high volume of SYNs packets without SYN-ACKs. This goes along with the requirement.		
57	15.6.8	13.2	MTCS Clause 13.2.4(a) states that an automated/real-time monitoring tool be implemented and even though, the scope of implementation is not defined, it can be assumed that such tools are generally implemented on external-internet facing systems to thwart any DDOS/defacement attacks. This goes along with the requirement and could be considered as included.	Included (needs further verification)	The principle behind the control is to protect systems from defacement and DDOS attacks. MTCS Clause 13.2.4 mentions about having an automated/real-time tool for monitoring. It can be assumed that such monitoring activities are generally carried out on external- facing systems due to the limitation of resources. This needs further verification.
58	15.6.9	13.1,13.4	Process of tracking and monitoring of all access to the network resources and system components, shall be established by CSP. Log retention procedure shall be established by CSP.	Included	N.A
59	15.7.1	14.2	Requirements and audit procedures to prevent malicious	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			code threats, shall be implemented by CSP.		
60	15.7.2	14.2	Requirements and audit procedures to prevent malicious code threats, shall be implemented by CSP.	Included	N.A
61	15.7.3	14.2	Requirements and audit procedures to prevent malicious code threats, shall be implemented by CSP.	Included	Although there was no mention of scanning being carried out periodically in the MTCS, detection was highlighted.
62	15.8.1	12.5	Controls and procedures to protect data loss and destruction by other tenants or by CSP authorised agents, should be established by CSP.	Included	N.A
63	15.8.2	-	According to the ISO/IEC 27002 ISMS COP Clause 12.3.1 (c), the backups should be stored offsite, a sufficient distance away, to escape any damage from disaster at the main site. The need for backup tapes to be stored offsite should have been considered during risk assessment and for implementation. As this is control is explicitly stated in ISO/IEC 27002 ISMS COP Clause 12.3(c), it could be considered as included.	Included (needs further verification)	ISO/IEC 27002 ISMS COP Clause 12.3.1 (c), explicitly mentions that the backups should be stored offsite, a sufficient distance away, to escape any damage from disaster at the main site. Rotating backup tapes offsite, helps is to protect the data in the event of fire, flood at the main information processing facility. This needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
64	15.8.3	21.3	A process to test and validate business continuity and disaster recovery plans to ensure effectiveness of recovery requirements, and staff's ability to execute emergency and recovery procedures, should be established by CSP.	Included	It is assumed that sensitive information including personal data, will be encrypted even if the media is to be stored onsite even if the media is to be stored onsite.
65	15.8.4	12.8	Secure disposal and decommissioning procedures for hardcopies, media and equipment, should be established and implemented by CSP.	Included	N.A
66	15.11.1	12.5	Controls and procedures to protect data loss and destruction by other tenants or by CSP authorised agents, should be established by CSP.	Included	N.A
67	16.2.1	22.1	Registration and the approval process in granting and modifying privileged rights to administrators of cloud services (e.g. applications, systems, databases, network configurations and sensitive data and functions), shall be established by CSP.	Included	N.A
68	16.2.2	22.1	Registration and approval process in granting and modifying privileged rights to administrators of cloud services (e.g. applications, systems, databases, network	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			configurations and sensitive data and functions), shall be established by CSP.		
69	16.2.3	22.2	Proper protection against system compromise shall be undertaken by CSP.	Included	It is assumed that administrator account refer all types of privileged users including but not limited to, power user, operator and root.
70	16.2.5	22.1	According to the ISO/IEC 27002: 2013 ISMS COP Clause 9.2.3(c), record of all privileges allocated should be maintained and privileged access should not be granted until authorized. The need for emergency access management should have been considered during risk assessment and implemented. As the control is explicitly stated in ISO/IEC 27002 ISMS COP, it could be considered as included.	Included (needs further verification)	The principle behind this control is for effective tracking and control over emergency access/privileged accounts and prevent their misuse. This is explicitly mentioned in ISO/IEC 27002:2013 ISMS COP Clause 9.2.3 (c). This needs further verification.
71	16.2.6	22.8	Logging via native system logs, application logs, for all administration activities (Clause 12), shall be undertaken by CSP.	Included	N.A
72	16.3.1	22.1,23.1	Duties and areas of responsibilities should be segregated by CSP, to reduce unauthorized or	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			unintentional modification or misuse of information assets. A formal user registration to grant, modify and restrict user access to the cloud services (applications, systems, databases and sensitive data/functions), shall be established by CSP.		
73	16.3.3	14.1	Configuration standards for all system components and network devices (virtualised images, snapshots and hypervisor), should be developed by CSP.	Included	N.A
74	16.3.4	22.13	Service and application accounts shall be created in accordance with requirements and audit procedures, by CSP.	Included	N.A
75	16.4.1	23.3	The password allocation process involving secure user selection of passwords, shall be implemented by CSP.	Included	N.A
76	16.4.2	23.3	The password allocation process involving secure user selection of passwords, shall be implemented by CSP.	Included	N.A
77	16.4.3	22.5	Regular changes to passwords based on the risk assessments and sensitivity of the system and data, should be ensured by CSP.	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
78	16.4.4	22.13	Service and application accounts shall be created in accordance with requirements and audit procedures, by CSP.	Included	This is a very special requirement as exemption is needed for service account.
79	16.4.5	22.2, 23.3, 22.5	Password controls to administrative accounts based on the risk assessments and sensitivity of systems, shall be enforced by CSP. The password allocation process involving secure user selection of passwords, shall be implemented by CSP. Regular changes to passwords based on the risk assessments and sensitivity of the system and data, should be ensured by CSP.	Included	N.A
80	16.4.6	23.5	Procedures should be established by CSP, for requirements and procedures pertaining to user password reset and first-logon change.	Included	N.A
81	16.4.8	14.1, 23.6	Configuration standards for all system components and network devices (virtualised images, snapshots and hypervisor), should be developed by CSP.	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			User login credentials shall be protected by requirements and audit procedures and CSP shall ensure this.		
82	16.4.9	22.11, 23.6	Encryption (Clause 16) and security protocols for transmitting credentials for non-console administrative access based on the risk assessments and sensitivity of the system and data, shall be implemented by CSP. User login credentials shall be protected by requirements and audit procedures and CSP shall ensure this.	Included	It is assumed that the user credentials will be secured and passwords cannot be stored in clear-text on storage systems and audit logs.
83	16.5.2	14.2	Requirements and audit procedures to prevent malicious code threats, shall be implemented by CSP.	Included	Security controls would refer to anti-malware solutions that are capable of detecting, removing and protecting against common types of malicious software. These solutions must be current, actively running and generating audit trails.
84	16.5.3	23.2	Level requirements and audit procedures for user access to the cloud environment should be enforced by CSP.	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
85	16.6.1	Nil	Applicable as it is only a guideline.	Included	It is noted that this is not inline but since this is just a guideline, it will be accepted as compliant.
86	16.6.2	14.6, 22.9	Inactive sessions should be managed by CSP. Controls to manage sessions based on the risk assessments and sensitivity of the data/system, should be established by CSP.	Included	N.A
87	16.6.3	22.9	Controls to manage sessions based on the risk assessments and sensitivity of the data/system, should be established by CSP.	Included	N.A
88	16.7.1	Nil	Applicable as it is only a guideline.	Included	It is not mentioned in the requirement that sensitive health information (SHI) and/or personal data should be masked or removed when printed on hardcopy reports or sent electronically. However, this is only a "should" within the policy statement. This is to note that this is not inline but since this is just a guideline, it will be accepted as compliant.
89	16.7.2	22.9	Controls to manage sessions based on the risk assessments and	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			sensitivity of the data/system, should be established by CSP.		
90	17.1.1	16.1	Policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities should be established by CSP.	Included	N.A
91	17.2.1	16.1	Policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities should be established by CSP.	Included	N.A
92	17.2.2	-	Organisation should have identified and implemented the control for the need for output data to be validated to ensure that it is correct and appropriate since it is explicitly identified in ISO/IEC 27002 ISMS COP Clause 14.2.5 (other information), which mentions application development should consider secure engineering techniques, which include data validation, for output interfaces, for consideration.	Included	N.A
93	17.3.1	-	ISO/IEC 27002: 2013 ISMS COP Clause 12.5.1(a) explicitly mentions that the updating of operational software should be undertaken by	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			trained administrators with authorization from management. Organisation should have identified and implemented the control for restricting access to operational software.		
94	17.3.2	16.4	Process to ensure source code security shall be established by CSP.	Included	N.A
95	17.3.3	20.4	Development, test and production environments shall be separated by CSP, to reduce the risk of unauthorised changes or access to the system.	Included	N.A
96	17.3.4	20.4	Development, test and production environments shall be separated by CSP, to reduce the risk of unauthorised changes or access to the system.	Included	There is an assumption here - the requirement specifies that restriction is needed but within the levels, they are not mentioned.
97	17.4.1	14.1	Configuration standards for all system components and network devices (virtualised images, snapshots and hypervisor), should be developed by CSP.	Included	N.A
98	17.4.2	14.7	System security parameters, should be configured by CSP, to prevent misuse of services and protocols.	Included	MTCS specifies enabling only the necessary and secure services. It would have the same meaning as the policy statement negated.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
99	17.4.3	15.1	Although MTCS Clause 15.1 mentions that vulnerability assessment must be conducted when there are significant changes and at least once a month, there was no mention on performing assessment prior to commissioning. However, as this is considered baseline and any vulnerabilities not patched before commissioning with pose a significant risk to the system. Therefore due to these assumptions, this could be considered as included.	Included (needs further verification)	Assumptions can be made that this is baseline and the system would inherit more issues if not patched prior to commissioning. This needs further verification.
100	17.4.4	15.2	Although MTCS Clause 15.2.4(a) mentions that penetration testing is conducted at least twice annually, with at least one test executed by a qualified third party and must be conducted when there are significant changes in infrastructure, application upgrades or modifications, there was no mention on performing assessment prior to commissioning.	Included (needs further verification)	Assumptions can be made that this is baseline and the system would inherit more issues not rectified prior to commissioning. This needs further verification.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			However, as this is considered baseline and any issues not rectified before commissioning with pose a significant risk to the system. Therefore due to these assumptions, this could be considered as included.		
101	17.4.5	20.5	A patch management process, incorporating level requirements and audit procedures, should be started by CSP.	Included	N.A
102	17.4.6		Applicable as assumption that secure coding is done.	Included	It is assumed that the only way to prevent common coding vulnerability is to perform secure coding.
103	17.5.1	17.1	While the requirement states that cryptographic techniques shall be used to protect the confidentiality, integrity and authenticity of information collected, processed and stored on IT systems, MTCS Clause 17.1 mentions about the usage of encryption, which is one of the cryptographic techniques. While no mention is made of the other cryptographic techniques like digital signing, it is assumed	Included	Encryption is one of the cryptographic techniques in protecting data confidentiality. However, these techniques can also protect the integrity of data. It is assumed that policies of such would have also considered the other uses of cryptography.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			that such techniques would have been considered before.		
104	17.5.2	17.2	Encryption shall implemented by CSP, wherever applicable.	Included	It is assumed that channel encryption includes all types of networks.
105	17.6.1	17.3	Key management procedures addressing all components of the lifecycle (generation, distribution, utilisation, storage, archiving, replacement and destruction of the keying material), should be established by CSP.	Included	N.A
106	17.6.3	17.3	Key management procedures addressing all components of the lifecycle (generation, distribution, utilisation, storage, archiving, replacement and destruction of the keying material), should be established by CSP.	Included	N.A
107	17.6.4	17.3	Key management procedures addressing all components of the lifecycle (generation, distribution, utilisation, storage, archiving, replacement and destruction of the keying material), should be established by CSP.	Included	N.A
108	17.6.5	17.3	Key management procedures addressing all components of the lifecycle (generation, distribution, utilisation, storage, archiving, replacement and destruction of	Included	It is assumed that there is a requirement to securely destroy the key, when an IT system is decommissioned and data is no longer required.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
			the keying material), should be established by CSP.		
109	18.1.1	11.3	An Information Security Incident process should be established by CSP.	Included	N.A
110	18.2.2	11.3	An Information Security Incident process should be established by CSP.	Included	N.A
111	18.2.3	11.3	An Information Security Incident process should be established by CSP.	Included	It is assumed that Incident reporting captures the description of the incident, data/time of incident discovered, actions taken immediately upon discovery, extent of the damage, type of system involved, contact information of reporting personnel via its reporting process.
112	18.2.4	11.1	An information security incident response plan and procedures to respond to incidents in a timely fashion, should be implemented and maintained by CSP.	Included	It is assumed that the investigation includes the identification of the source of attack and perpetrators involved
113	19.1.1	21.2	CSP shall develop and implement BCP and DR plans.	Included	N.A
114	19.1.2	21.1	A Business Continuity Planning (BCP) framework for the required cloud services, should be developed, maintained and communicated by CSP.	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
115	19.1.3	21.2	CSP shall develop and implement BCP and DR plans.	Included	N.A
116	19.1.4	21.1	CSP shall devise a recovery strategy so that recovery needs and implementation will be aligned.	Included	
117	19.1.5	21.3	A process to test and validate business continuity and disaster recovery plans to ensure effectiveness of recovery requirements, and staff's ability to execute emergency and recovery procedures, should be established by CSP.	Included	N.A
118	19.1.6	21.3	A process to test and validate business continuity and disaster recovery plans to ensure effectiveness of recovery requirements, and staff's ability to execute emergency and recovery procedures, should be established by CSP.	Included	N.A
119	19.1.7	21.3	A process to test and validate business continuity and disaster recovery plans to ensure effectiveness of recovery requirements, and staff's ability to execute emergency and recovery procedures, should be established by CSP.	Included	N.A

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
120	19.1.8		Applicable as record keeping requirement assumed to be in practice.	Included	As part of the record keeping requirement for all standards requirement, this will be assumed to be in practice.
121	20.1.1	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	It is assumed that the CSP shall adhere to the following minimum legislation including Personal Data Protection Act, Computer Misuse and Cybersecurity Act. Evidence Act and Electronic Transaction Act.
122	20.2.2	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	N.A
123	20.3.1	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	N.A
124	20.3.2	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	N.A
125	20.3.3	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	N.A
126	20.4.1	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	It mentions that they need to declare.

S/N	Policy Statement	MTCS Clause	Brief description on its applicability	L3 Gaps	Comments
127	20.5.2	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	It mentions that they need to declare
128	20.6.1	10.1	Documentation pertaining to the level requirements and audit procedures, shall be identified, created and maintained by CSP.	Included	It mentions that they need to declare.