INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS) Implementation Guideline Report

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

December 2014

Revision History

Revision Date	Version	Updated by	Description
December 2014	Ver. 1.0	IDA	Initial Release

Disclaimer

The information provided in this Implementation Guideline Report is for general information purposes only. The Implementation Guideline 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 Implementation Guideline Report. The Working Group and IDA are entitled to add, delete or change any information in the Implementation Guideline Report at any time at their absolute discretion without giving any reasons.

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

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

The experts of the Working Group are affiliated with:

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

The Multi-tiered Cloud Security cross-certification Focus Group on MTCS SS to ISO/IEC 27001:2013 was appointed by IDA to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

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

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

Contents

1 Normative References

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

- **Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS).** MTCS SS aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS SS provides relevant cloud computing security practices and controls for cloud users, Auditors and certifiers to understand cloud security requirements, and for public Cloud Service Providers to strengthen and demonstrate the cloud security controls in their cloud environments.
- **ISO/IEC 27001:2013** *Information technology -- Security techniques -- Information security management system requirements*. ISO/IEC 27001 is the international standard for information security management which defines a set of controls and requirements to establish, implement, operate, monitor, review, maintain and improve an information security management system (ISMS). ISO/IEC 27001:2013 Standard is the second edition of the standard and replaces the first edition ISO/IEC 27001:2005 Standard. This standard benefits entities in allowing them to demonstrate commitment and compliance via the adoption of this standard.

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

2 Purpose of Document

This Implementation Guideline Report is the second report in the set of three (3) documents to support cross-certification between MTCS SS and ISO/IEC 27001:2013. The purpose of each document is described in the diagram below.

Gap Analysis Report	Implementation Guideline Report	Audit Checklist Report
The purpose of the Gap Analysis Report is to provide an overview of the differences between the requirements listed in MTCS SS and the ISO/IEC 27001:2013 Standard. The information provided in this document aims to assist entities that are MTCS SS certified to adopt the ISO/IEC 27001:2013 Standard. Cloud Service Providers that are MTCS SS certified will have to comply with the requirements stated in ISO/IEC 27001:2013 Standard that are not fully covered in MTCS SS.	The purpose of the Implementation Guideline Report is to assist Cloud Service Providers that are MTCS SS certified to implement the ISO/IEC 27001:2013. The guidelines in the report are generic and need to be tailored to each Cloud Service Provider's specific requirements.	The purpose of the Audit Checklist Report is to guide Auditors, including internal audit function, ISO/IEC 27001:2013 Certification Bodies and external audit bodies in understanding additional requirements beyond MTCS SS. From the Cloud Service Providers' perspective, this document serves as a general guide for them to understand the scope covered in ISO/IEC 27001:2013 certification audit when the scope of MTCS SS audit overlaps with scope of the ISO/IEC 27001:2013 audit.

3 Intended Audience

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

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

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 – Scope
- Section 7 – Tips on Using this Implementation Guideline Report
- Section 8 – Implementation Guidelines

5 Terms and Definitions

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

6 Scope

In order to assist Cloud Service Providers that are MTCS SS certified to adopt the ISO/IEC 27001:2013, we have developed this Implementation Guideline Report for the gaps identified in Gap Analysis Report, which are classified as “INCREMENTAL” or “NEW”.

For ease of reference, the description of the gap classifications is listed below. For the full report on the gap analysis, refer to the Gap Analysis Report.

Gap Classification	Description
INCREMENTAL	Indicates the clauses in ISO/IEC 27001:2013 that are stated with more details than the corresponding sections in clauses in the MTCS SS. In general, the requirements are classified as "INCREMENTAL" if the required enhancements on the existing MTCS SS characteristics are not costly or onerous in nature.
NEW	Indicates the clauses in ISO/IEC 27001:2013 that are absent, or stated with significantly more details than the corresponding sections and clauses in the MTCS SS. In general, the requirements are classified as "NEW" if there may be a material financial cost to meet the relevant ISO/IEC 27001:2013 requirement, additional controls to be included in the audit checklist and / or the effort is relatively onerous.

Note that requirements that were listed as “INCLUDED” in the Gap Analysis Report will not be discussed in this document.

Gap Classification	Description
INCLUDED	Indicates the clauses in ISO/IEC 27001:2013 that are equally represented in MTCS SS.

7 Tips on Using this Implementation Guideline Report

This document is meant to help Cloud Service Providers who are MTCS SS Levels 1, 2 or 3 certified and are implementing or planning to implement the ISO/IEC 27001:2013. The guidelines are generic and Cloud Service Providers will need to tailor the suggested guidelines to their specific requirements.

Cloud Service Providers should refer to the implementation guidelines listed for the MTCS SS Level that they are certified for if they are looking to be certified in ISO/IEC 27001:2013. For example, if a Cloud Service Provider is certified for MTCS SS Level 3, the provider should only refer to implementation guidelines listed in Section 8.1 ’MTCS SS Levels 1-3‘. If the Cloud Service Provider is certified to MTCS SS Level 1, they should refer to corresponding guidelines in Section 8.1 ‘MTCS SS Levels 1-3‘, Section 8.2 ‘MTCS SS Levels 1-2‘ and Section 8.3 ‘MTCS SS Level 1‘.

While there may be multiple instances of activities stated in various sections of the ISO/IEC 27001:2013, Cloud Service Providers may opt to combine such activities into a single activity with a scope covering the relevant areas in order to optimise resources or improve efficiency.

For example, activities related to reviews and audits are mentioned in ISO/IEC 27001:2013 Clauses 6.2 ‘Information security objectives and planning to achieve them’ and 9.3 ‘Management review’. As such, Cloud Service Providers can choose to structure their reviews in a single session, or across multiple sessions.

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

8 Implementation Guidelines

This document is meant to help Cloud Service Providers who are MTCS SS certified and are implementing or planning to implement ISO/IEC 27001:2013. The guidelines are generic and need to be tailored to each service provider's specific requirements.

8.1 MTCS SS Levels 1-3

This section summarises the implementation guidelines for gaps identified between all MTCS SS Levels and ISO/IEC 27001:2013.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
5 Leadership		
5.2 Policy		
5.2(para.1b) Incremental	MTCS SS requires the establishment of an information security policy. However, as part of the policy, it does not explicitly specify the need to include information security objectives. As part of the organisation's information security policy, Cloud Service Providers shall include information security objectives or provide a framework to develop information security objectives. For details of establishing and achieving the information security objectives, refer to ISO/IEC 27001:2013 Clause 6.2.	While an information security policy (MTCS SS Clause 6.4) is able to establish the direction of the organisation, the inclusion of information security objectives in the information security policy is not explicitly mentioned.
6 Planning		
6.1 Actions to address risks and opportunities		
6.1.2 Information security risk assessment		
6.1.2(para.1b) Incremental	MTCS SS only implies and does not specifically require consistent, valid and comparable results from risk assessments, or identification of risk owners. The Cloud Service Provider should update existing documentation to ensure that information security risk assessments achieve	While ensuring periodic risk assessments produce consistent, valid and comparable results is not mentioned, inclusion of specific types of risks (MTCS SS Clause 8.2.2(c)) in assessments, and associated documentation can assist in the production of consistent, valid and comparable results.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
6.1.2(para.1c2) Incremental	the abovementioned criteria. Changes can include: • provision of a standard template document with relevant columns on previous results and risk owners; • process to compare previous results during risk assessments; and • add information on asset risk owners and previous assessments to the existing risk register.	While identification of risks (MTCS SS Clause 8.1) can be observed, the identification of risk owners is not specifically mentioned.
6.1.3 Information security risk treatment		
6.1.3(para.1f) Incremental	MTCS SS does not specifically cover the requirement for risk owners to approve the security risk treatment plan and the acceptance of residual information security risks. The Cloud Service Provider shall obtain the risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks during the information security risk treatment process. This can be captured in sign-off forms, risk registers, etc. This is to help ensure that the risk owners understand what is required of them or the organisation (e.g., resources, procedures, policies) in order to address the risk and understand the impact of any residual information security risks.	Risk owner's approval of the information security risk treatment plan and acceptance of the residual information security risks are not formally mentioned.
6.2 Information security objectives and planning to achieve them		
6.2(para.1) Incremental	MTCS SS does not specifically require the information security objectives to be established at relevant functions and levels. The Cloud Service Provider shall establish information security objectives at relevant functions (e.g., IT, finance, HR, operations) and levels (e.g., operational, managerial, senior management) throughout the organisation.	MTCS SS does not specifically cover the establishment of information security objectives at relevant functions and levels.
7 Support		
7.2 Competence		
7.2(para.1c) Incremental	MTCS SS does not specifically require actions to be taken to develop competency and to evaluate the effectiveness of those actions. The Cloud Service Provider shall take actions such as training, etc. to develop relevant competency and thereafter implement measures to evaluate the effectiveness of the actions.	The need for developing competence and thereafter implementing controls to measure its effectiveness is not specifically mentioned in the MTCS SS.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
7.2(para.1d) Incremental	MTCS SS does not cover the need to retain appropriate documentation as evidence of the personnel's competencies in performing information security related tasks. The Cloud Service Provider shall retain appropriate documentation, upon hire and during the course of employment, as evidence of its personnel's competency. These personnel include person(s) doing work that may affect the organisation's information security performance. Examples of documented evidence include, but are not limited to, training certificates, academic transcripts and external security certifications. While retaining documentation of personnel's competency, Cloud Service Providers should also take note of the requirements for documented information in ISO/IEC 27001:2013 Clause 7.5 Documented Information.	The need for the appropriate documentation of the competency of person(s) doing work affecting the organisation's information security performance is not specifically mentioned in the MTCS SS.
7.5 Documented information		
7.5.2 Creating and updating		
7.5.2(para.1b) Incremental	MTCS SS does not cover the specific formats and media for the documentation of information. The Cloud Service Provider shall ensure appropriate formats (e.g., language, software version, graphics) and media (e.g., paper, electronic) of various documented information on information security system management (e.g., results of risk assessments, evidence of competencies, policies) are created and maintained. This is to help ensure that an appropriate format of documented information is readily available, as required.	There is no mention of specific formats and media, that is required to bring consistency and completeness across all the documentation of information in the MTCS SS.
9 Performance evaluation		
9.2 Internal audit		
9.2(para.1a2) Incremental	The Cloud Service Provider shall extend the audit committee's scope to include requirements mentioned in ISO/IEC 27001:2013 Clause 9.2 to ensure conformance to the standard.	Scope of audit committee does not specifically include ISO/IEC 27001:2013.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
9.2(para.2f) Incremental	While MTCS SS requires the establishment of an audit committee, it does not specifically require the reporting of audit results to relevant management. The Cloud Service Provider shall report audit results to relevant management (e.g., audit committee, senior management). This is to ensure that managers know what is lacking or requires attention in the area they are overseeing and thus, can take appropriate actions to address any non-compliance or gaps.	There is no explicit mention of reporting audit results to relevant management though the establishment of an audit committee and the identification of participants involved in the meeting or committee, their respective job functions and the reporting relationship (MTCS SS Clause 6.6) could imply so.
9.3 Management review		
9.3(para.2a) Incremental 9.3(para.2b) Incremental 9.3(para.2c1) Incremental 9.3(para.2c2) Incremental 9.3(para.2c3) Incremental	The Cloud Service Provider shall include, in its management reviews of the organisation's information security management system: • Status of actions from previous management reviews. • Changes in external and internal issues that are relevant to the organisation's environment. • Feedback of the performance of the organisation's information security. As listed in the ISO/IEC 27001:2013, such feedbacks include, but are not limited, to the following: ○ trends in nonconformities and corrective actions, ○ trends in monitoring and measurement results, ○ trends in audit results; and ○ trends in fulfilment of information security objectives. • Feedback (e.g., ease of use, time spent on routine ISMS tasks) from interested parties / stakeholders (e.g., customers[1], personnel[2]). • Risk assessment results and the risk treatment plan status. • Opportunities for continual improvement[3]. • Output[4] of its management reviews of the organisation's information security management system include decisions related to continual improvement opportunities and decisions for changes). • Retain documentation[5] as evidence of the management reviews. Examples of such	While there are elements of management reviews (MTCS SS Clauses 6.2 and 6.3) specific topics relevant to the information security management system in management reviews are not mentioned.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
9.3(para.2c4) Incremental 9.3(para.2d) Incremental 9.3(para.2e) Incremental 9.3(para.2f) Incremental 9.3(para.3) Incremental 9.3(para.4) Incremental	documentation include, but are not limited to: ○ minutes of meetings; and ○ to-do lists. [1] Example(s) of feedback from customers / users as potential stakeholders: • ease of use of service after the implementation of a security control; and • response time of service after the implementation of a security control. [2] Example(s) of feedback from personnel as potential stakeholders: • time taken to maintain / monitor a security control; and • difference in effort for performance of task after a change in the ISMS. [3] Examples of opportunities for continual improvement include, but are not limited to: • reviewing results of actions taken from a cost saving perspective, • subscribe to news / updates relevant to ISMS; and • participate in seminars / forums where industry experts / enthusiasts share ISMS ideas and innovations. [4] Examples of outputs of management reviews include, but are not limited to: • deciding on which opportunity to take advantage of, • updated policy, • additional resources to acquire; and • new system to implement. [5] While retaining documentation of these management reviews, Cloud Service Providers should also take note of the requirements for documented information in ISO/IEC 27001:2013 Clause 7.5 Documented Information.	
10 Improvement		
10.1 Nonconformity and corrective action		

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
10.1(para.3f) Incremental	MTCS SS does not specifically require documentation of the nature of nonconformities and the actions taken to deal with the nonconformities. The Cloud Service Provider shall retain documentation about the nature of the nonconformities related to the information security management and any corrective actions taken and the results. This is to ensure that the organisation and its personnel know what has been identified and implemented previously, and the effectiveness of the actions. This is done to reduce duplicate efforts in attempting something that has been performed before. While retaining documentation of these management reviews, Cloud Service Providers should also take note of the requirements for documented information in ISO/IEC 27001:2013 Clause 7.5 Documented Information.	MTCS SS does not explicitly mention controls to retain documented evidence for the following: • nonconformities, • details of corrective action; and • results of corrective action.
10.1(para.3g) Incremental		
A.9 Access Control		
A.9.4 System and application access control		
A.9.4.1 Incremental	MTCS SS states that access related controls should be implemented; however it does not explicitly require an access control policy. The Cloud Service Provider shall define an access control policy to ensure that access to information and application system functions is granted only to the authorised personnel.	While there are elements of access related controls in MTCS SS, specific requirement related to access control policy is not mentioned.

8.2 MTCS SS Levels 1-2

In addition to the guidelines mentioned in the previous section, for the gaps between all MTCS SS Levels and ISO/IEC 27001:2013, this section summarises the implementation guidelines for additional gaps identified between MTCS SS Levels 1 and 2, and ISO/IEC 27001:2013. Note that this section is applicable to Cloud Service Providers that are MTCS SS Levels 1 and 2 certified.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps
7 Support		
7.5 Documented information		
7.5.3 Control of documented information		
7.5.3(para.2d) Incremental	MTCS SS does not explicitly require storage protection for documented information. The Cloud Service Provider shall address appropriately, with technical or organisational controls, the storage and preservation of the documented information. Examples of these controls include, but are not limited to, access controls for storage facilities, continuous review and signoff for documents and the cryptographic controls for information in-transit. See MTCS SS Clause 12 for Data Governance requirements.	While there are elements of storage and data protection in MTCS SS, details of storage protection, redundancy and testing are not mentioned in sufficient details except in Level 3 of MTCS SS Clauses 12.5 and 12.6.
9 Performance evaluation		
9.2 Internal audit		
9.2(para.1a2) New	The Cloud Service Provider shall extend the audit committee's scope to include requirements mentioned in ISO/IEC 27001:2013 Clause 9.2 to ensure conformance to the standard.	Scope of audit committee does not specifically include ISO/IEC 27001:2013.
10 Improvement		
10.1 Nonconformity and corrective action		
10.1(para.1d) Incremental	MTCS SS does not specify that effectiveness of the mitigating controls should be evaluated. The Cloud Service Provider shall implement controls to review the effectiveness of any corrective action taken to mitigate the gaps.	While the control to measure the effectiveness is explicitly included for Level 3 in MTCS SS, it is not defined for Levels 1 and 2.

8.3 MTCS SS Level 1

In addition to the guidelines mentioned in the previous section, for the gaps between MTCS SS Levels 2 and 3 and ISO/IEC 27001:2013, this section summarises the implementation guidelines for additional gaps identified specific to MTCS SS Level 1. Note that this section is applicable to Cloud Service Providers that are MTCS SS Level 1 certified.

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
6 Planning		
6.1 Actions to address risks and opportunities		
6.1.2 Information security risk assessment		
6.1.2(para.1e1) Incremental	While risk assessment controls can be observed in MTCS SS, it does not specifically require referencing to risk criteria that were defined at an earlier stage, or any prioritisation in risks. As part of the evaluation of information security risks, the Cloud Service Provider shall compare the results of the risk analysis with the risk criteria (i.e., a term of reference / attribute to describe the significance of the risk to the organisation, and determine if the risk is to be accepted or mitigated) that was established in ISO/IEC 27001:2013 Clause 6.1.2 a.	While MTCS SS covers risk assessments (MTCS SS Clauses 8.1 and 8.2), risk criteria is only specifically mentioned in Level 2 of MTCS Clauses 8.1 and 8.4, and risk prioritisation is only specifically mentioned in Level 2 of MTCS SS Clauses 8.1, 8.3 and 8.4.
6.1.2(para.1e2) Incremental	An example of a risk criterion would be for cases where potential breaches are common. This is to help ensure that the risk criteria established at an earlier stage is still relevant or require a review. The Cloud Service Provider shall also prioritise the risks analysed for risk treatment. This is to help ensure that risks that were identified as high priority receive the most attention and are resolved / mitigated within the shortest possible timeframe. In addition, Cloud Service Providers can also include the information on risk criteria and priority as part of the risk register documentation.	
6.2 Information security objectives and planning to achieve them		

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
6.2(para.2b) Incremental 6.2(para.2c) Incremental	MTCS SS does not specifically require the details required by ISO/IEC 27001:2013 for information security objectives. The Cloud Service Provider shall: • Add to the existing processes or procedures the measurement of these information security objectives. This is to help ensure that information security objectives that were established at an earlier stage can be tracked and used as an indicator on how the organisation is performing in terms of information security. Examples of these processes or procedures include, but are not limited to, the development of metrics and key indicators of information security performance, and the regular review of the information security objectives based on the metrics and indicators. • Consider relevant information security requirements, risk assessments results and risk treatments results; while establishing the information security objectives. This is to help ensure that what the organisation wants to achieve is aligned with what they are doing or how they are performing.	MTCS SS does not specifically cover security objectives including: • Development of metrics to measure information security objectives is not mentioned. To be able to determine the effectiveness of the policy (MTCS SS Clause 6.5) would imply some elements of measurements. • While there are no explicit mentions of taking into account applicable information security requirements, and results from risk assessment and risk treatment in the development of information security objectives; elements of them can be observed from the organisation's approach to managing information security (MTCS SS Clause 6.4), and reviewing and updating of the information security policy (MTCS SS Clause 6.5), and checking against results of risk assessment is only specifically mentioned in MTCS SS Clause 8.3 Level 2.
7 Support		
7.5 Documented Information		
7.5.3 Control of documented information		
7.5.3(para.2f) Incremental	MTCS SS does not specifically define the control for retention of documented information. The Cloud Service Provider shall define controls for the retention of the documented information.	MTCS SS Clause 12 mentions controls related to secure data according to it classification, however it does not explicitly mention about the retention of the information.
8 Operation		
8.3 Information security risk treatment		
8.3(para.2) Incremental	MTCS SS does not specifically require the documentation of the results of information security risk treatments. The Cloud Service Provider shall retain appropriate documentation of the results of information security risk treatments, which can be done via inclusion of results of risk treatments in the existing risk register. While retaining documentation of these results, Cloud Service Providers should also take note of the requirements for documented information in ISO/IEC 27001:2013 Clause 7.5 Documented Information.	Documentation is mentioned broadly in MTCS SS Clauses 6.1 and 6.3. However, there is no explicit mention about the documentation of the results from information security risk treatment in the MTCS SS until Level 2 of MTCS SS Clause 8.4.
A.8 Asset management		
A.8.2 Information classification		

ISO/IEC 27001:2013 clause	Implementation guidance	Additional context on gaps identified
A.8.2.1 New	MTCS SS does not cover the classification of information. The Cloud Service Provider shall establish an information classification process in order to classify its assets appropriately according to the assets' importance to the organisation. Some factors to take into consideration during the process include, but are not limited to: • legal requirements; • monetary value of the information; and • criticality and sensitivity of the information.	Classification of information is not mentioned in Level 1 of Clause 12.1 in MTCS SS. No applicable Level 1 controls.
A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements		
A.18.1.4 Incremental	While MTCS SS require high level compliance to regulatory requirements, it does not specifically require the protection of personally identifiable information. The Cloud Service Provider shall establish controls (e.g., technical controls) and procedures (e.g., requiring consent to be given by information owners, disclosure of personal identifiable information) to ensure the privacy and protection of personally identifiable information, as required in relevant legislation and regulation (e.g., Personal Data Protection Act (PDPA) in Singapore).	High level compliance to regulatory requirements (MTCS SS Clause 10.1) was mentioned but not specific to the privacy and protection of personally identifiable information.

<End of Implementation Guideline Report>