INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS)
Audit Checklist 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 Audit Checklist Report is for general information purposes only. The Audit Checklist 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 Audit Checklist Report. The Working Group and IDA are entitled to add, delete or change any information in the Audit Checklist 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 Audit Checklist Report is the third 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.

This Audit Checklist Report and associated audit procedures are intended to help MTCS SS certified Cloud Service Providers carry out trial cross-certification with auditors / Certification Bodies for ISO/IEC 27001:2013. As such, this document does not include audit related information on recommended audit timeline and competency criteria for auditors.

Note that this report only covers gaps identified in Gap Analysis Report. It is recommended for Cloud Service Providers and Certification Bodies to view the complete set of audit procedures provided by ISO/IEC 27001:2013 or other relevant documents.

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

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

4 Scope

This report only covers gaps identified between MTCS SS and ISO/IEC 27001:2013 as listed in the Gap Analysis Report. The main goal of the listed audit procedures is to aid Cloud Service Providers to cross certify from MTCS SS to ISO/IEC 27001:2013.

The Audit Checklist Report includes 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 number of 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 number of 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 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 number of clauses in the ISO/IEC 27001:2013 that are equally represented in the MTCS SS.

5 Document Structure

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

- Section 6 – Terms and Definitions
- Section 7 – Tips on Using this Audit Checklist Report
- Section 8 – Audit Checklist

6 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.

7 Tips on Using this Audit Checklist Report

Section 8 includes the corresponding audit procedures required for gaps identified in Gap Analysis Report. This list is intended to guide auditors and Cloud Service Providers certified in MTCS SS Levels 1, 2 or 3, in auditing and adopting ISO/IEC 27001:2013. From the Cloud Service Providers' perspective, this document serves as a general guide for them to understand the incremental scope covered in ISO/IEC 27001:2013 certification audits when already MTCS SS Levels 1, 2 or 3 certified.

Cloud Service Providers should refer to the audit checklist listed for the MTCS SS Level that they were certified for if they are looking to be cross-certified for ISO/IEC 27001:2013. For example, if a Cloud Service Provider has been certified in MTCS SS Level 3, they should refer to the audit checklist listed in Section 8.1 'MTCS SS Levels 1-3'. If the CSP is certified to MTCS SS Level 1, they should refer to 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'. The concept above also applies to auditors, including internal audit function and ISO/IEC 27001:2013 external auditors.

It is recommended for Cloud Service Providers to refer to the Implementation Guideline Report while using this document. It is also recommended for Cloud Service Providers and Certification Bodies to view the complete set of audit procedures provided by ISO/IEC 27001:2013 or other relevant documents.

Descriptions of the respective columns for the checklists in Sections 8.1, 8.2 and 8.3 are listed below:

Note that a "√" in the respective columns indicates whether the control requires document review, system review or visual inspection recommended as part of the audit activities to be performed by the assessors.

Column	Column description
Organisational Control	Auditors shall gather evidence of the performance of organisational controls through review of the records of performance of controls, interviews and observations. Main questions to answer are: 1. Does the organisation have documented controls? 2. Is the role and responsibility clear and complete?
Technical Control / Visual Control Review	Auditors shall gather evidence on the performance of technical / physical controls through system review, which can be performed via a set of technical activities. Examples of these technical activities include, but are not limited to the following: 1. Inspection of system, or system or device configurations / settings 2. Physical inspection of controls Main questions to answer are: 1. Are controls implemented as documented? 2. Do controls meet ISO 27001 requirements?

Effectiveness Review	Auditors shall visually inspect controls on site or at the location to evaluate their effectiveness. This means that it is not sufficient to review the respective documentation on paper or through interviews – the auditors need to verify the controls at the location (if necessary) where it is implemented. Evaluation and review of testing results produced from previous tests performed by personnel from the Cloud Service Provider or third-parties engaged by the Cloud Service Provider. Main questions to answer are: 1. Are the controls implementation effective to the risk level? 2. Do controls implemented achieve their purpose?

While selecting and deciding on the audit activities to be performed, Certification Bodies shall take into consideration the impact of non-compliance to the Cloud Service Provider's operations, the importance of the specific security control specified in MTCS SS and the cost of performing the audit activity. From this point of view, the audit activities for cross-certification with MTCS SS Level 3 are more demanding relative to MTCS SS Levels 2 and 1.

8 Audit Checklist

8.1 MTCS SS Levels 1-3

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

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
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. Determine if information security objectives or a framework to develop information security objectives have been included in the Cloud Service Provider's information security policy. For details of establishing and achieving the information security objectives, refer to ISO/IEC 27001:2013 Clause 6.2.	√		√
6 Planning				
6.1 Actions to address risks and opportunities				
6.1.2 Information security risk assessment				

6.1.2(para.1b)
Incremental
 	
6.1.2(para.1c2)
Incremental
	MTCS SS only implies and does not specifically require consistent, valid and comparable results from risk assessments, or identification of risk owners.
	
	Determine if processes / procedures have been established to ensure that the results of risk assessments are consistent, valid and comparable. Also, determine if the risk owners have also been identified by the Cloud Service Provider as part of the risk register (paper-based or via system).
	
	Some of the possible processes / procedures include, but are not limited to:
	• preparing standard document templates for assessors; and
	• providing past reports / results to assessors as a reference.
		√		√

6.1.3 Information security risk treatment				

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
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. Determine if appropriate approval (manual or via system) has been obtained from the risk owners for the information security risk treatment plan and acceptance of the residual information security risks.	√		√
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. Determine if information security objectives have been established by the Cloud Service Provider at relevant functions (e.g., IT, finance, HR, operations) and levels (e.g., operational, managerial, senior management) throughout the organisation.	√		√
7 Support				
7.2 Competence				
7.2(para.1c) Incremental	MTCS SS does not specifically require actions to be taken to develop or acquire the necessary information security related competency for personnel performing tasks relevant to information security, and to evaluate the effectiveness via implementation of controls. Determine if the Cloud Service Provider has taken actions to develop relevant competency and thereafter implemented measures to evaluate the effectiveness of the actions (i.e., training needs and definition of learning outcomes).	√		√
7.2(para.1d) Incremental	MTCS SS does not cover the need to retain appropriate documentation as evidence of the personnel's competency in performing information security related tasks. Determine if appropriate documentation of personnel competency has been retained via manual filing or knowledge base by the Cloud Service Provider upon hire and during the course of employment. Examples of documented evidence include, but are not limited to, training certificates, academic transcripts and external security certifications.	√		√
7.5 Documented information				
7.5.2 Creating and updating				

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
7.5.2(para.1b) Incremental	MTCS SS does not cover the specific formats and media for the documentation of information. Determine if various documented information on information security management system (e.g., results of risk assessments, evidence of competencies, policies) have been created and maintained in: • appropriate formats (e.g., language, software version, graphics); and • appropriate media (e.g., paper, electronic).	√		√
9 Performance evaluation				
9.2 Internal audit				
9.2(para.1a2) Incremental	MTCS SS Clause 6.1.4, a Level 3 clause, requires Cloud Service Providers to have a valid ISO/IEC 27001 certification for the ISMS. However, ISO/IEC 27001:2013 was not released at the point of MTCS SS' release. As such, the gap for MTCS SS Level 3 certification is classified "Incremental" against ISO/IEC 27001:2013 clause 9.2(para.1a2) while MTCS SS Level 2 and Level 1 certifications are classified "New" against the same clause. As part of the audit scope, determine if gaps identified in the Gap Analysis Report have been addressed by the Cloud Service Provider.	√		√
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. Determine if audit results have been reported to relevant management (e.g., audit committee, senior management) via appropriate channels and methods.	√		√
9.3 Management review				
9.3(para.2a) Incremental	While MTCS SS requires the implementation of performance of management reviews, the inclusion of topics as specified in ISO/IEC 27001:2013 Clause 9.3(para.2) is not mentioned. Determine / verify of the following have been included as items for discussions in management reviews: • status of actions from previous management reviews; • changes in external and internal issues relevant to the organisation's information security environment; • feedback of the performance of the organisation's information security, • feedback (e.g., ease of use, time spent on routine ISMS tasks) from interested parties /	√	√	√
9.3(para.2b) Incremental				
9.3(para.2c1) Incremental				

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
9.3(para.2c2) Incremental	stakeholders (e.g., customers[1], personnel[2]); • risk assessment results and status of the risk treatment plan; • opportunities[3] for continual improvement; • outputs[4] of the management reviews include decisions related to continual improvement (e.g., deciding on which opportunity to take advantage of) and decisions for changes (e.g., updated policy, additional resources to acquire, new system to implement) to the information security; management system; and • documentation of management reviews have been retained as evidence. [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.			
9.3(para.2c3) Incremental				
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				
10 Improvement				
10.1 Nonconformity and corrective action				
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. Determine if the nature of	√		√

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
10.1(para.3g) Incremental	nonconformities related to the information security management system have been documented by the Cloud Service Provider via paper or system, including effectiveness of the actions to reduce duplicated efforts.			
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. Determine if the Cloud Service Provider has defined an access control policy to ensure that access to information and application system functions is granted only to the authorised personnel.	√	√	

8.2 MTCS SS Levels 1-2

In addition to the audit guidance mentioned in the previous section, this section summarises the audit procedures 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	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
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, redundancy and testing for documented information. Determine if appropriate technical or organisational controls have been established by the Cloud Service Provider to address the storage and preservation of documented information, including system rules. 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.	√	√	
9 Performance evaluation				
9.2 Internal audit				

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
9.2(para.1a2) New	MTCS SS does not require the conformance to ISO/IEC 27001:2013 since MTCS SS was released before ISO/IEC 27001:2013. As part of the audit scope, determine if gaps identified in the Gap Analysis Report have been addressed by the Cloud Service Provider.	√	√	
10 Improvement				
10.1 Internal audit				
10.1(para.1d) Incremental	MTCS SS does not specify that effectiveness of the mitigating controls should be evaluated. Determine if the Cloud Service Provider reviews the effectiveness of any corrective action taken to mitigate the gaps via review of policies, procedures, existing reports and results, and system configuration.	√	√	

8.3 MTCS SS Level 1

In addition to the audit guidance mentioned in the previous section, this section summarises the audit procedures 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	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
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. Determine if risk criteria derived from ISO/IEC 27001:2013 Clause 6.1.2(a) was compared against the results of risk analysis, with focus on critical security areas (e.g., scenarios where potential breaches are common), to determine the relevance of the risk criteria. Also, determine if risks identified were prioritised for treatment based on their criticality in day-to-day operations of cloud services. This information can be included as part of the risk register information, or a separate document, depending on the organisation.	√		
6.1.2(para.1e2) Incremental				
6.2 Information security objectives and planning to achieve them				

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
6.2(para.2b) Incremental	MTCS SS does not specifically require the details specified in ISO/IEC 27001:2013 on information security objectives e.g., development of metrics to measure effectiveness. Determine if the Cloud Service Provider has: • Included in the existing processes or procedures the measurement of effectiveness for these information security objectives. • Utilise any systems / tools to track and manage metrics mentioned above. • Considered relevant information security requirements, risk assessments results and risk treatments results; while establishing the information security objectives.	√	√	
6.2(para.2c) Incremental				
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. Determine if the Cloud Service Provider has defined controls for the retention of the documented information, and consider reviewing system rules on document retention and archival virtually.	√	√	
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. Determine if appropriate documentation of the results of information security risk treatments have been retained by the Cloud Service Provider. Also, verify that the requirements for documented information in ISO/IEC 27001:2013 Clause 7.5 Documented Information have been taken into consideration.	√	√	
A.8 Asset management				
A.8.2 Information classification				
A.8.2.1 New	MTCS SS does not cover the classification of information. Determine if an information classification process and/or system has been established to classify assets appropriately according to the assets' criticality to the organisation or the operation of the cloud services.	√	√	

ISO/IEC 27001:2013 clause	Audit Guidance	Organisational Control	Technical Control / Visual Control Review	Effectiveness Review
A.18 Compliance				
A.18.1 Compliance with legal and contractual requirements				
A.18.1.4 Incremental	MTCS SS requires high level compliance to regulatory requirements at Level 1 but specific requirement for the protection of personally identifiable information are not mentioned. Determine if controls, procedures and/or system rules have been established by the Cloud Service Provider 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).	√	√	

<End of Audit Checklist Report>