
INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

# Multi-Tiered Cloud Security Standard for Singapore (MTCS SS) Audit Checklist Report

*For cross-certification from MTCS SS to Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)*

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 and CSA STAR 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 |
| Aloysius Cheang | Cloud Security Alliance APAC |
| Daniele Catteddu | Cloud Security Alliance EMEA |

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.
- **CSA Cloud Control Matrix (CCM) v3.0.** The Cloud Security Alliance (CSA) launched the Security, Trust & Assurance Registry (STAR) initiative at the end of 2011, in order to improve security posture in the cloud. CSA CCM v3.0 was defined to support this framework. It provides the guidance on necessary security controls for a Cloud Service Provider to assess the maturity of their security framework.
- **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.

# 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 CSA STAR based on CCM v3.0 and ISO/IEC 27001:2013. The purpose of each document is described in the diagram below.

This Audit Checklist Report and the associated audit procedures are intended to help MTCS SS certified Cloud Service Providers in performing a trial cross-certification with auditors / certification bodies on CSA STAR. As such, this document does not include audit related information on areas such as the recommended audit timeline and competency criteria for auditors.

Note that this document only covers the gaps that have been identified in the Gap Analysis Report. It is recommended for Cloud Service Providers and auditors to view the audit procedures listed in the STAR Certification Auditing the Cloud Control Matrix (CCM) document, dated 08 August 2013.

| 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 CSA STAR.<br><br>The information provided in this document aims to assist entities that are MTCS SS certified to adopt CSA STAR. Cloud Service Providers that are MTCS SS certified will have to comply with the requirements stated in CSA STAR 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 CSA STAR.<br><br>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, CSA STAR certification bodies and external audit bodies in understanding additional requirements beyond MTCS SS.<br><br>From the Cloud Service Providers' perspective, this document serves as a general guide for them to understand the scope covered in CSA STAR certification audit when the scope of the MTCS SS audit overlaps with scope of CSA STAR. |

# 3 Intended Audience

This Audit Checklist Report is intended for Cloud Service Providers that are MTCS SS Levels 1, 2 or 3 certified and interested in obtaining CSA STAR certification for the following scenarios:

**Cloud Service Providers that are ISO/IEC 27001:2013 certified**

As CSA STAR certification is based upon achieving ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, this report assumes that Cloud Service Providers that are MTCS Levels 1, 2 or 3 certified are also ISO/IEC 27001:2013 certified (Please refer to https://cloudsecurityalliance.org/star/certification/ for details on CSA STAR certification requirement).

**Cloud Service Providers that are not ISO/IEC 27001:2013 certified**

This report also caters for Cloud Service Providers that are not ISO/IEC 27001:2013 certified but are interested in obtaining CSA STAR certification. Cloud Service Providers that fall under this category can follow a 2-step approach, as listed below, to obtain the CSA STAR certification.

Step 1: Refer to the Audit Checklist Report for cross-certification from MTCS SS to ISO/IEC 27001:2013.
Step 2: Refer to the audit checklist in this report.

The application of the audit checklist from the 2-step approach above will enable Cloud Service Providers that are not ISO/IEC 27001:2013 certified to obtain CSA STAR certification.

This report is also intended to guide auditors, including internal auditors, CSA STAR certification bodies and external audit bodies on the differences between MTCS SS and the CSA STAR, and the required audit procedures.

# 4 Scope

The Audit Checklist Report includes the gaps identified in the 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 MTCS SS that are stated with more details than the corresponding sections in clauses in CSA STAR[1]. 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 MTCS SS that are absent, or stated with significantly more details than the corresponding sections and clauses in CSA STAR[1]. In general, the requirements are classified as "NEW" if there may be material financial cost to meet the relevant CSA STAR[1] requirement, additional controls to be included in the audit checklist and / or the effort is relatively onerous. |

[1]CSA STAR includes clauses in CSA CCM v3.0 and ISO/IEC 27001:2013.

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 CSA STAR[1] that are equally represented in MTCS SS. |

[1]CSA STAR includes clauses in CSA CCM v3.0 and ISO/IEC 27001:2013.

# 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

Cloud-related terms used in this report are defined in CSA CCM v3.0, MTCS SS and ISO/IEC 27001:2013.

# 7 Tips on Using this Audit Checklist Report

Section 8 includes the corresponding audit procedures required for gaps identified in the Gap Analysis Report. This list is intended to guide auditors and Cloud Service Providers certified in MTCS SS Levels, in auditing and adopting CSA STAR. From the Cloud Service Providers' perspective, this document serves as a general guide for them to understand the incremental scope that is covered in CSA STAR certification audits when Cloud Service Providers are already MTCS SS 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 CSA STAR. For example, if a Cloud Service Provider has been certified in MTCS SS Level 3, the provider should refer to the audit checklist 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 the corresponding audit checklist in Section 8.1 'MTCS SS Levels 1-3' and Section 8.2 'MTCS SS Level 1'. The concept above also applies to auditors, including internal and external auditors.

It is recommended for Cloud Service Providers to refer to the Implementation Guideline Report and Gap Analysis Report while using this document. Descriptions of the respective columns for the checklists in Sections 8.1 and 8.2 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.<br><br>Main questions to answer are:<br>1. Does the organisation have documented controls?<br>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:<br>1. Inspection of system, or system or device configurations / settings<br>2. Physical inspection of controls<br><br>Main questions to answer are:<br>1. Are controls implemented as documented?<br>2. Do controls meet CSA STAR 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.<br><br>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.<br><br>Main questions to answer are:<br>1. Are the controls implemented effective to the risk level?<br>2. Do controls implemented achieve their purpose? |

While selecting and deciding on the audit activities to be performed, auditors / 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 CSA STAR and the cost of performing the audit activity. From this point of view, the audit activities for cross-certification from MTCS SS Level 3 are more demanding relative to MTCS SS Levels 2 and 1.

# 8 Audit Checklist

As CSA STAR certification is based upon achieving both ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, identified gaps between CSA CCM and MTCS SS that are fulfilled by ISO/IEC 27001:2013 are not included in this report. Refer to the Gap Analysis Report for more details.

For Cloud Service Providers that are not ISO/IEC 27001:2013 certified but are interested in obtaining CSA STAR certification should follow the 2-step approach as described in Section 3 'Intended Audience'.

## 8.1 MTCS SS Levels 1-3

This section summarises the audit procedures for gaps identified between all MTCS SS Levels and CSA STAR.

| CSA CCM V3.0 Control ID / Control Name | Audit Guidance | Organisational Control | Technical Control / Visual Control Review | Effectiveness Review |
|---|---|---|---|---|
| **AIS Application & Interface Security** | | | | |
| AIS-02 Customer Access Requirements Incremental | MTCS SS does not require all identified security, contractual, and regulatory requirements to be addressed prior to grant of access to customers. Determine if the Cloud Service Provider has implemented the appropriate policies, procedural and technical measures to address and remediate all identified requirements for customer access as mentioned in AIS-02 before granting customers access to data, assets and information systems. | √ | √ | √ |
| **Infrastructure & Virtualization Security** | | | | |
| IVS-05 Management - Vulnerability Management Incremental | MTCS SS does not specify any details on the types of security vulnerability assessment tools or services used by the Cloud Service Provider. Determine if the Cloud Service Provider and associated third parties are using security vulnerability assessment tools or services that address vulnerabilities in the virtualisation technologies used for the provision of cloud services. | | √ | √ |
| IVS-10 VM Security - vMotion Data Protection Incremental | MTCS SS does not cover specific requirements relating to data protection during the migration of physical servers, applications, or data to virtualised servers. Determine if the Cloud Service Provider has used secured and encrypted communication channels when migrating the components mentioned in IVS-10 to virtualised servers. Also, determine if the Cloud Service Provider has used a network that is segregated from the production environment for such migrations. | | √ | √ |

| CSA CCM V3.0 Control ID / Control Name | Audit Guidance | Organisational Control | Technical Control / Visual Control Review | Effectiveness Review |
|---|---|---|---|---|
| IVS-12 Wireless Security<br>Incremental | MTCS SS relies on network segmentation and physical security; hence it does not specifically require the capability to detect unauthorised wireless network devices and timely disconnection from the network. Determine if the Cloud Service Provider has implemented the appropriate policies, procedural and technical measures to detect unauthorised devices connected to the network. In addition, determine if controls are in place to promptly disconnect from the wireless network any unauthorised device. | √ | √ | √ |
| **Interoperability & Portability** | | | | |
| IPY-01 APIs<br>Incremental | MTCS SS does not specifically require the use of open and published APIs. Determine if the Cloud Service Provider and associated third parties are using open and published APIs to maximise interoperability between components. | √ | | √ |
| IPY-03 Policy & Legal<br>New | MTCS SS does not require providers to satisfy cloud user requirements for application and data interoperability and portability criteria as mentioned in IPY-03. Determine if the Cloud Service Provider has implemented the appropriate policies and procedures to satisfy cloud users' requirements for the areas as mentioned in IPY-03. | √ | | √ |
| IPY-05 Virtualization<br>New | MTCS SS does not require providers to use an industry endorsed virtualisation platform and standard virtualisation formats to facilitate interoperability. Determine if the Cloud Service Provider has implemented the appropriate policies and procedures that dictate the use of only industry endorsed virtualisation platforms and standard virtualisation formats to maximise interoperability. In addition, determine if the Cloud Service Provider has documented all custom changes made to hypervisors and solution-specific virtualisation hooks and make the documents available for cloud users' review. | √ | √ | √ |
| **Mobile Security** | | | | |
| MOS-10 Device Management<br>New | MTCS SS does not require the deployment of a centralised mobile device solution to manage mobile devices that have access to company data. Determine if the Cloud Service Provider has implemented an appropriate centralised mobile device management solution and has deployed the solution to all mobile devices that have access to company data. | | √ | √ |

| CSA CCM V3.0 Control ID / Control Name | Audit Guidance | Organisational Control | Technical Control / Visual Control Review | Effectiveness Review |
|---|---|---|---|---|
| MOS-12 Jailbreaking and Rooting<br>New | MTCS SS does not prohibit the circumvention of built-in security controls on mobile devices. Determine if the Cloud Service Provider has established and documented a mobile device policy and if it clearly states clauses that prohibit bypassing security controls on mobile devices such as jailbreaking and rooting. Verify that such prohibition is enforced through technical controls on the device or through a centralised device management system (i.e., CSA CCM Control MOS-10). | √ | √ | √ |
| MOS-17 Policy<br>Incremental | MTCS SS does not require the establishment and documentation of a mobile device policy. Determine if the Cloud Service Provider has established and documented a mobile device policy and if it is clearly stating clauses requiring<br>• BYOD personnel to perform backups of data;<br>• prohibition of usage of unapproved application stores; and<br>• usage of anti-malware software, where supported. | √ | | √ |
| MOS-18 Remote Wipe<br>New | MTCS SS does not require mobile devices that have access to company data to be available for remote wipe by the company's corporate IT. Determine if the Cloud Service Provider has implemented the appropriate policies, procedural and technical measures to allow mobile devices for remote wipe by the company's corporate IT. | √ | √ | √ |
| MOS-19 Security Patches<br>Incremental | MTCS SS does not require mobile devices that have access to company data to be remotely validated by the organisation for latest security patches. Determine if the Cloud Service Provider has implemented the appropriate policies, procedural and technical measures for remote validation of latest security patches for mobile devices. In addition, verify that all mobile devices having access to company data have the latest available security-related patches installed. | √ | √ | √ |

## 8.2 MTCS SS Level 1

This section summarises the audit procedures for gaps identified between MTCS SS Level 1 and CSA STAR.

| CSA CCM V3.0 Control ID / Control Name | Audit Guidance | Organisational Control | Technical Control / Visual Control Review | Effectiveness Review |
|---|---|---|---|---|
| **Data Security & Information Lifecycle Management** | | | | |
| DSI-05 Information Leakage Incremental | MTCS SS Level 1 does not cover data leakage. Determine if the Cloud Service Provider has implemented the appropriate procedural and technical measures to protect data in storage and data in transit to prevent data leakage. Such measures include, but are not limited to:<br>• access control on storage devices and information processing facilities;<br>• encryption before storage and before transit; and<br>• regular reviews and security testing. | √ | √ | |
| **Governance and Risk Management** | | | | |
| GRM-01 Baseline Requirements Incremental | MTCS SS Level 1 does not specify a required frequency to perform compliance review against the security baseline requirements. Determine if the Cloud Service Provider has reviewed and reassessed its compliance with security baseline requirements at least on an annual basis. | √ | | |

<End of Audit Checklist Report>