iDA SINGAPORE

INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

# Multi-Tiered Cloud Security Standard for Singapore (MTCS SS) Implementation Guideline 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 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 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 Implementation Guideline Report is the second report in the set of three (3) documents to assist Cloud Service Providers that are MTCS SS certified to adopt CSA STAR based on CCM v3.0 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 CSA STAR.<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>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>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 Implementation Guideline 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:

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

As the 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).

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

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.

<u>Step 1:</u> Refer to the Implementation Guideline Report for cross-certification from MTCS SS to ISO/IEC 27001:2013.
<u>Step 2:</u> Refer to the implementation guidelines in this report.

The application of the implementation guidelines 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 the internal audit function, certification bodies and external audit bodies, on the control differences between CSA STAR and MTCS SS, and the corresponding implementation guidelines.

# 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

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

# 6 Scope

In order to assist entities that are MTCS SS certified to adopt CSA STAR, 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 CSA STAR[1] that are stated with more details than the corresponding sections in clauses in 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 CSA STAR[1] that are absent, or stated with significantly more details than the corresponding sections and clauses in MTCS SS. 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.

# 7 Tips on Using this Implementation Guideline Report

This document is meant to help Cloud Service Providers who are MTCS SS certified in Levels 1, 2 or 3 and are implementing or planning to implement CSA STAR. The guidelines are generic and Cloud Service Providers will need to tailor them 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 CSA STAR. For example, if a Cloud Service Provider is certified in 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 in MTCS SS Level 1, they should refer to the corresponding guidelines in Section 8.1 ‘MTCS SS Levels 1-3’ and Section 8.2 ‘MTCS SS Level 1’.

While there may be multiple instances of certain activities (e.g., training, reviews) in various sections of CSA CCM, 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.

# 8 Implementation Guidelines

As the 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 implementation guidelines for gaps identified between MTCS SS Levels 1, 2 or 3, and CSA STAR.

| CSA CCM V3.0 Control ID / Control Name | Implementation Guidance | Additional information on gaps identified (MTCS SS Level 1 - 3) |
|---|---|---|
| **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 granting access to customers. The Cloud Service Provider shall ensure that all identified requirements for customer access as mentioned in AIS-02 are addressed and remediated prior to granting customers access to data, assets, and information systems. | While MTCS SS defines the controls to address security, contractual and regulatory requirements in general; it does not specifically require that these identified requirements must be addressed prior to granting access to customers.<br>Note: Gap is also found when mapping MTCS SS to ISO/IEC 27001:2013. Refer to Clause A.9.4.1 in ISO/IEC 27001:2013. |
| **Infrastructure & Virtualization Security** | | |

| CSA CCM V3.0 Control ID / Control Name | Implementation Guidance | Additional information on gaps identified (MTCS SS Level 1 - 3) |
|---|---|---|
| IVS-05 Management - Vulnerability Management<br>Incremental | MTCS SS does not require the types of security vulnerability assessment tools or services used by the Cloud Service Provider. The Cloud Service Provider and associated third-parties, if development is outsourced, should leverage security vulnerability assessment tools or services that address vulnerabilities in the virtualisation technologies used for the provisioning of cloud services. | While MTCS SS covers vulnerability management for virtualised technologies in general, it does not specifically require the security vulnerability assessment tools or services used by the Cloud Service Provider to manage vulnerabilities of virtualisation to accommodate the virtualisation technologies used. |
| IVS-10 VM Security - vMotion Data Protection<br>Incremental | MTCS SS does not cover specific requirements relating to data protection during the migration of physical servers, applications, or data to virtualised servers. The Cloud Service Provider shall have policies, procedural and technical measures in place to ensure that secured and encrypted communication channels are used when migrating the components to virtualised servers as mentioned in IVS-10. Also, where possible, the Cloud Service Provider shall also use a network segregated from production environment for such migrations. | While MTCS SS covers channel encryption in general for channels used for transmission of sensitive information, it does not specifically require the usage of secure and encrypted channels for migrating physical servers, applications, or data to virtualised servers. |
| 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. The Cloud Service Provider shall have policies, procedural and technical measures in place to detect unauthorised devices connected to the network. Upon detection, the unauthorised devices shall be disconnected promptly from the wireless network. | 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. |
| **Interoperability & Portability** | | |
| IPY-01 APIs<br>Incremental | MTCS SS does not specifically require the use of open and published APIs. In addition to conducting software development in accordance with industry standards and practices, the Cloud Service Provider shall use open and published APIs to maximise interoperability between components. | While MTCS SS covers software development in accordance with industry standards and practices, it does not specifically require utilisation of open and published APIs to maximise interoperability. |

| CSA CCM V3.0 Control ID / Control Name | Implementation Guidance | Additional information on gaps identified (MTCS SS Level 1 - 3) |
|---|---|---|
| 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. The Cloud Service Provider shall have policies and procedures in place to satisfy cloud users' requirements for application and data interoperability and portability criteria as mentioned in IPY-03. | MTCS SS does not require providers to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability. It also does not require the providers to satisfy customer (tenant) requirements on portability for application development and information exchange, usage and integrity persistence. |
| IPY-05 Virtualization<br>New | MTCS SS does not require providers to use industry endorsed virtualisation platform and standard virtualisation formats to facilitate interoperability. The Cloud Service Provider shall ensure that only industry endorsed virtualisation platform and standard virtualisation formats are used.<br><br>The Cloud Service Provider shall also document all custom changes made to hypervisors and solution-specific virtualisation hooks and make the documents available for cloud users' review. | MTCS SS does not require providers to use an industry-recognised virtualisation platform and standard virtualisation formats (e.g., OVF) to help ensure interoperability between varying environments and infrastructures. It also does not require providers to have documented custom changes made to any hypervisor in use, and have all solution-specific virtualisation hooks available for customer 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. The Cloud Service Provider shall implement a centralised mobile device management solution that will be deployed to all mobile devices that have access to company data. | MTCS SS does not require a centralised, mobile device management solution to be deployed to all mobile devices used to store, transmit, or process company data. |
| MOS-12 Jailbreaking and Rooting<br>New | MTCS SS does not prohibit the circumvention of built-in security controls on mobile devices. The Cloud Service Provider shall establish and document a mobile device policy that includes clauses that prohibit bypassing built-in security controls on mobile devices such as jailbreaking and rooting. The requirement shall be enforced through technical controls on the device or through a centralised device management system (i.e., CSA CCM Control MOS-10). | MTCS SS does not require the prohibition of circumvention of built-in security controls on mobile devices. |

| CSA CCM V3.0 Control ID / Control Name | Implementation Guidance | Additional information on gaps identified (MTCS SS Level 1 - 3) |
|---|---|---|
| MOS-17 Policy<br>Incremental | MTCS SS does not require the establishment and documentation of a mobile device policy. The Cloud Service Provider shall establish and document a mobile device policy that includes 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. | While MTCS SS requires policies for acceptable usage in general, it does not specifically require a BYOD policy covering requirements for the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and use of anti-malware software. |
| 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. The Cloud Service Provider shall have the appropriate policies, procedural and technical measures in place.<br><br>All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT. | MTCS SS does not require mobile devices to have the capability to be remotely wiped by the company's corporate IT or shall have all company-provided data wiped 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. The Cloud Service Provider shall have policies, procedural and technical measures in place for mobile devices to allow for remote validation by the organisation for latest security patches. The Cloud Service Provider shall ensure that all mobile devices having access to company data have the latest available security-related patches installed upon general release. | While MTCS SS requires the establishment of patch management procedures in general, it does not specifically require mobile devices to allow remote validation to download the latest security patches by company IT personnel. |

## 8.2 MTCS SS Level 1

This section summarises the implementation guidelines for additional gaps identified specific to MTCS SS Level 1. Note that this section is only applicable to Cloud Service Providers that are MTCS SS Level 1 certified.

| CSA CCM V3.0 Control ID / Control Name | Implementation Guidance | Additional information on gaps identified (MTCS SS Level 1) |
|---|---|---|
| **Data Security & Information Lifecycle Management** | | |
| DSI-05 Information Leakage<br>Incremental | MTCS SS Level 1 does not cover data leakage. The Cloud Service Provider shall have procedural and technical measures in place 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. | MTCS SS Level 1 does not have requirements that specifically address data leakage.<br>Note: Gap is also found when mapping MTCS SS to ISO/IEC 27001:2013. Refer to Clause 7.5.3(para.2d) in ISO/IEC 27001:2013. |
| **Governance and Risk Management** | | |
| GRM-01 Baseline Requirements<br>Incremental | MTCS SS Level 1 does not specify a frequency for the compliance checks. The Cloud Service Provider shall review and reassess its compliance with security baseline requirements at least on an annual basis. | While MTCS SS Level 1 requires compliance checks to be done regularly, it does not specify the frequency of such checks. |

<End of Implementation Guideline Report>