INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS584:2015) Audit Checklist Report

For bridging MTCS SS584:2015 to ISO/IEC 27018:2014

April 2016

Revision History

Revision Date	Version	Updated by	Description
April 2016	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 (as listed in this document), 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 Harmonisation Working Group on bridging MTCS SS584:2015 to ISO/IEC 27018:2014 was a joint project formed by the Infocomm Development Authority (IDA) and Microsoft Singapore to assist in the preparation of this report. It comprises the following members:

	Name	
Project Sponsors		
	Dr. Hing-Yan Lee	IDA
	Erick Stephens	Microsoft
Facilitator:	Tao Yao Sing	IDA
Secretary:	Dr. Aaron Thor	IDA
Members:	Darryn Lim	Microsoft
	Gary Lim	Microsoft
	Alfred Wu Hoi	Microsoft
	Antony Ma	IDA

The Multi-Tiered Cloud Security Harmonisation Focus Group on bridging MTCS SS584:2015 to ISO/IEC 27018:2014 was formed by IDA to assist in providing professional insights, verification and endorsement of this report. It comprises the following experts:

Dave Cheng	Certification International (Singapore)
Ros Oh	DNV Business Assurance Singapore
Lee Lai Mei	SGS International Certification Services Singapore
Christian Weidinger	TÜV Rheinland Singapore
Chris Ng	TÜV SÜD PSB
James Liu	Amazon Web Services
Alex Ng/Alan Ng	ClearManage
Edmund Tan	Acclivis Tech
Kenneth Yeo	Ascenix
Terence Ang	M1
Alan Woo	NewMedia Express
David Loke	ReadySpace
Septika/Sendang	Telin Singapore
Michael Mudd	Open Computing Alliance
Dr. Lam Kwok Yan	Association of Information Security Professionals
Aloysius Cheang	Cloud Security Alliance
John Lim	Information Systems Audit and Control Association
Dr. Chen Yuan Yuan	National University of Singapore
Prof. Anwitaman Datta	Nanyang Technological University
Jeffrey Tan	Deloitte
Tan Shong Ye	PricewaterhouseCoopers

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 report:

- Singapore Standard for Multi-Tiered Cloud Computing Security (MTCS SS584:2015 and hereinafter called MTCS). MTCS aims to encourage the adoption of sound risk management and security practices for cloud computing. MTCS 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 (CSPs) to strengthen and demonstrate the cloud security controls in their cloud environments.
- ISO/IEC 27018:2014 (hereinafter called ISO 27018) Information technology – Security Techniques- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect PII in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, ISO 27018 specifies guidelines based on ISO/IEC 27002:2013 (hereinafter called ISO 27002), taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

2. Purpose of Document

This Audit Checklist Report is the second report in the set of three (3) documents to support the harmonization between MTCS and ISO 27018. 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 and the ISO 27018 Standard. The information provided in this document aims to assist entities that are MTCS-certified to adopt the ISO 27018 Standard. CSPs that are MTCS-certified will have to comply with the requirements stated in ISO 27018 Standard that are not fully covered in MTCS.		The purpose of the Implementation Guideline Report is to assist CSPs that are MTCS-certified to implement the ISO 27018. The guidelines in the report will include recommendations on how to address or the close the gaps. However, the guidelines are generic and need to be tailored to each CSP's specific requirements.		The purpose of the Audit Checklist Report is to guide auditors, including internal audit function, ISO 27018 Certification Bodies and external audit bodies in understanding additional requirements beyond MTCS. From the CSPs' perspective, this document serves as a general guide for them to understand the scope covered in ISO 27018 certification audit when the scope of MTCS audit overlaps with scope of the ISO 27001 audit.

3. Intended Audience

This Audit Checklist Report is meant for following audience

- CSPs who are MTCS Level 2 or Level 3 certified who are interested in complying with ISO 27018.
- Auditors, including internal audit function, ISO 27001 Certification Bodies and external audit bodies on the differences between ISO 27018 Standard and MTCS.

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 Definition
- Section 6 – Approach
- Section 7 – Summary of findings
- Section 8 – Tips on using the Audit Checklist
- Section 9 – Audit Checklist

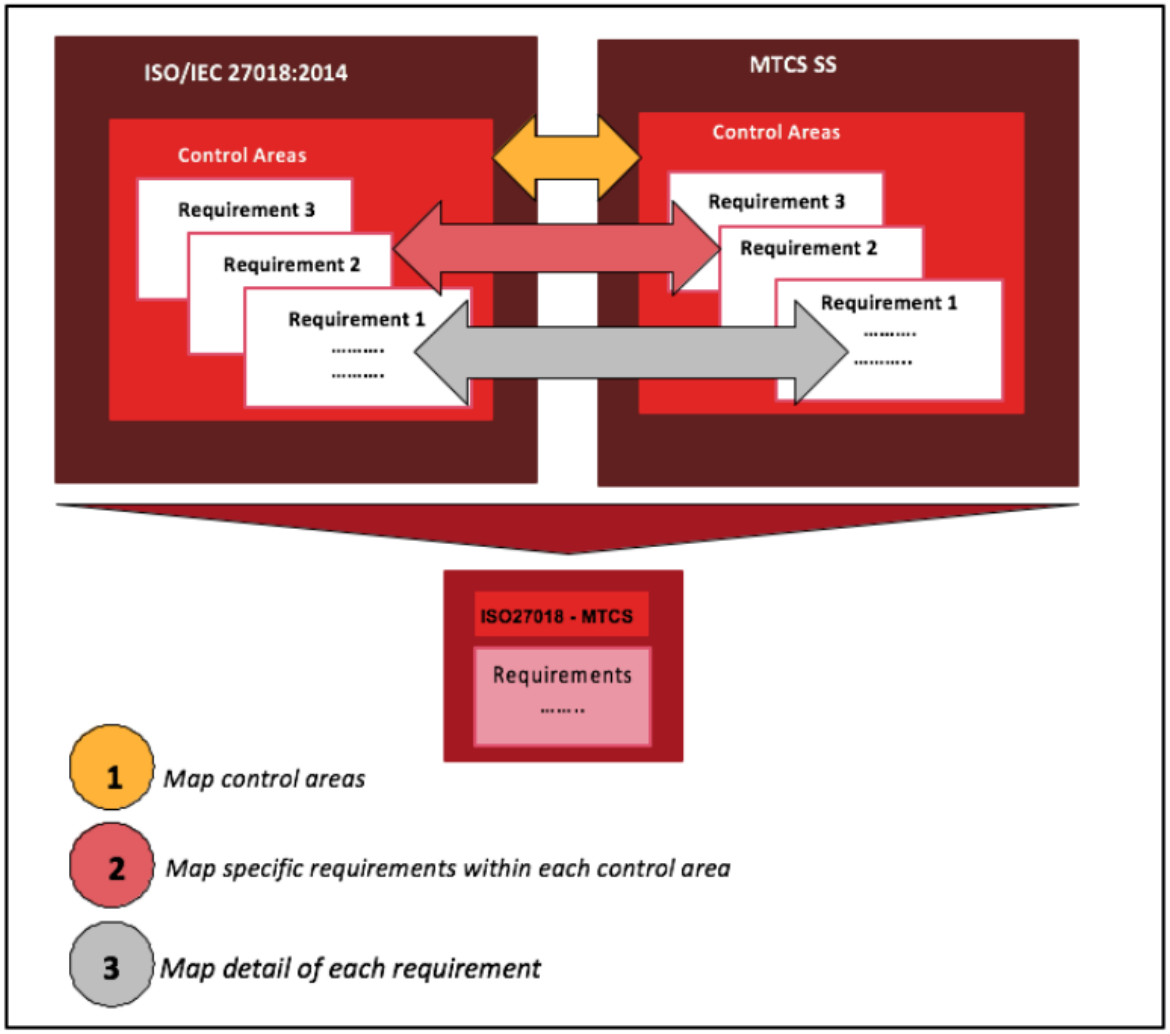
5. Terms and Definitions

All terms used within this report are derived from ISO 27018 and MTCS. The reader is advised to refer to the above-mentioned two documents in order to obtain the definitions if further clarity is needed. In case of conflicting terms and definitions provided within the two documents, MTCS terms and definitions will take precedence over ISO 27018.

6. Approach

In order to assist CSPs that are MTCS- certified to adopt ISO 27018, requirements listed in MTCS were mapped against equivalent requirements in ISO 27018. This followed a structured and systematic 3-step approach.

Note the mappings to ISO 27018 were only made for MTCS Level 2 and Level 3 requirements, as MTCS Level 1 requirements are only applicable for hosting of public information that does not include any PII.



7. Summary of Mapping

Of the 98 clauses in ISO 27018, only 39 clauses were found to include public cloud PII protection implementation guidance. Hence, only these 39 PII related clauses with breakdowns of the extent of coverage by MTCS are shown in table below, were considered for mapping between ISO 27018 and MTCS.

However, for completeness of mapping to other clauses, please refer to the Gaps Analysis Report and Implementation Guidelines Report on cross-certification from MTCS to ISO 27001, available from https://www.ida.gov.sg/programmes-partnership/small-and-mediumenterprises/initiatives/MTCS-Certification-Scheme

Coverage description	Number of PII clauses	Percentage of PII clauses (%)
The requirements in ISO27018 are not covered in MTCS	4	10.3
The requirements in ISO27018 are partly covered in MTCS, i.e. some gaps exist	19	48.7
The requirements in ISO27018 are fully covered in the MTCS, i.e. no gap exists.	16	41
Total:	39	100

8. Tips On Using This Audit Checklist Report

Section 8 highlights the corresponding audit procedures required for gaps identified in the Gap Analysis Report. This list is intended to guide auditors, including internal audit function, ISO 27018 Certification Bodies and external audit bodies in understanding additional requirements beyond MTCS SS. The document will serve as a general guide for CSPs to understand the scope covered in ISO 27018 certification audit when the scope of MTCS SS audit overlaps with scope of the ISO 27001 audit.

It is important for CSP to refer to the Implementation Guidelines Report and Gap Analysis Report while using this document. Descriptions of the respective columns for the Checklists are listed below: Note that a "√" in the respective columns indicates whether the control requires document review, system review or visual inspection as part of the audit activities to be performed by the assessors.

Column	Column Description
Organisational Control	Auditors shall obtain evidence of the performance of organisational controls through review of the records of performance of controls, interviews and observation. Main questions to answer are: 1. Does the organization have documented controls? 2. Is the role and responsibility clear, complete and being practiced/followed as documented?
Technical Control/ Visual Control Review	Auditors shall obtain 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 device configurations/settings 2. Physical inspection of controls Main questions to answer are: 1. Are controls implemented as documented? 2. Do controls meet stated requirements/control objectives?
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 on-site at the location (if necessary) where it is implemented.

	Evaluation and review for effectiveness of testing results produced from previous tests performed by personnel from the Cloud Service Provider or third-parties engaged by the CSP. Main questions to answer are: 1. Are the controls implemented effective to the risk level? 2. Do controls implemented achieve their purpose?

9. Audit Checklist

CSPs that are MTCS Level 2 or Level 3 certified and are interested in complying with ISO 27018 can view the Audit Checklist that need to be addressed in Tables 1 and 2, where the requirements of ISO 27018 are not covered or partially covered in MTCS SS respectively.

Table 1: The following requirements in ISO 27018 are not covered in MTCS SS

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
A1.1	Obligation to cooperate with rights of PII principals	MTCS has no matching clause(s) that state that the CSP should provide the cloud service customer with the ability to fulfil their obligation for exercising the PII principals' rights to access, correct and/or erase PII pertaining to them Determine if CSP has established polices on accessing, correcting and/or erasing PII in cloud systems based on PII principals' rights and also the corresponding processes (e.g. access control) to provision for such activities.		√		√
A2.1	Purpose Limitation	MTCS has no matching clause(s) that require that PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer. Determine if CSP has established polices to prevent the misuse of to-be-processed PII, resulting from a deviation from the stated purpose in the cloud service customer's contract, and was explicit in contractual terms with the cloud service customer in ensuring that there was no deviation from the stated purpose with regards to processing of the PII.		√		

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
A2.2	No commercial use	MTCS has no matching clause(s) that state that the PII processed under contract should not be used by the CSP for marketing and advertising without consent. Determine if CSP, has established polices to protect the PII being processed from misuse by the public cloud processor resulting from non-consensual marketing and advertising, and was explicit in contractual terms with the cloud service customer in ensuring that PII would not be used for marketing and advertising without consent.		√		
A5.1	Disclosure notification	MTCS has no matching clause(s) that state that the cloud service customer should be notified of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited Determine if CSP has established polices on the handling of legally binding requests with regards to the disclosure of PII and was explicit in contractual terms with the cloud service customer about disclosure notification.		√		

Table 2: The following requirements in ISO 27018 are partially in MTCS SS

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
5.1.1	Policies for Information Security	MTCS Clauses 9.22(a) and 9.33(a) does not explicitly state that CSP's Contractual agreements to clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and cloud service customer. Determine if CSP has identified and documented the roles and responsibilities of the customer as well as its sub-contractor.		√		
6.1.1	Information Security Roles and Responsibilities	MTCS Clauses 6.71 and 6.7.3(a) does not explicitly state that CSP should designate a contact point for Cloud Service Customer with regards to processing of PII under the contract Determine if CSP has identified and documented the roles and responsibilities of the contact point designate, with regards to the processing of PII, for the Cloud Service Customer.		√		
10.1.1	Policy on the use of cryptographic controls	MTCS Clauses 17.1.2, 17.2.2, 17.3.2, 17.3.3, 17.4.2 does not explicitly state that CSP should provide information to cloud service customer on the circumstances in which it uses cryptography to protect the PII being processed and any capabilities it provides that may assist the Cloud Service Customer in applying its own cryptographic protection. Determine if CSP has established polices in which cryptography is used to protect PII and the capabilities it provides that may assist the Cloud Service Customer in applying its own protection. Also, determine if there is a mechanism implemented to disseminate the policy to the cloud service customer.		√	√	√

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
11.2.7	Secure disposal or re-use of equipment	MTCS Clauses 12.8.2 and 12.9.3 do not explicitly state that storage media should be treated as though it contains PII, in cases of equipment re-use. Determine if CSP has established policies to enforce all storage media to be treated as containing PII to go through secure disk erasure prior to re-use. Also determine if there are established corresponding processes such as equipment re-use procedure etc., to provision for such activities.		√		√
12.1.4	Separation of development, testing and operation environments	MTCS Clauses 16.3.2 and 16.3.3 do not explicitly state that a risk assessment be undertaken for the use of PII, for testing purposes that cannot be avoided. Determine if CSP has performed risk assessment before using PII for testing purposes, if such testing is unavoidable.		√		√
12.3.1	Information Backup	MTCS Clauses 12.7.2 and 12.9.3 do not explicitly mention that multiple copies of data in physically and/or diverse locations must be stored, a documented maximum time-period within which data can be restored and reviews pertaining to the backup procedures to be conducted at planned intervals. Determine if CSP has enhanced their backup and restoration process to include how multiple copies of data in physical and/or diverse locations must be stored, a documented maximum time-period within which data can be restored and reviews pertaining to the backup procedures to be conducted at planned intervals.		√		√

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
13.2.1	Information transfer policies and procedures	MTCS Clauses 12.4 and 12.5 do not explicitly state that incoming/outgoing physical media containing PII to be recorded. Determine if CSP has enhanced policies on Asset Management by adding in the requirement that incoming/outgoing physical media containing PII is to be recorded. Also, determine if the corresponding processes such as Asset Movement process etc., have been enhanced to provision for such activities.		√		√
16.1.1	Responsibilities and procedures for security incidents	MTCS Clause 11 does not explicitly stipulate a review/examination/analysis of security incidents to determine if a data breach involving PII has occurred. Determine if the CSP has enhanced the information security incident management process by having additional steps to ascertain if a data breach of PII has occurred.		√		√
18.2.1	Independent Review of Information Security	MTCS Clause 10.2.2 does not explicitly state that the CSP should make independent evidence implementation and operation of information security available to Cloud Service Customers. Determine if CSP has made available to cloud service customers, independent evidence of the implementation and operation of information security. Also determine if CSP has implemented a mechanism/platform to make the independent evidence available to customers.		√	√	√
A4.1	Erase Temporary Files	MTCS Clauses 12.6.3 and 12.8.2 do not explicitly stipulate the erasure or destroying of temporary files	MTCS Clauses 12.6.3, 12.6.4 and 12.8.2 do not explicitly stipulate the erasure or destroying of temporary files	√	√	√

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
		and documents or that such erasure or destruction should be within a specified documented period. Determine if CSP has established policies that require the CSP to specifically destroy temporary files (e.g. cookies) and documents and also such erasure or destruction should be within a specified documented period. Also determine, if corresponding hardening guidelines have been established and applied to the applications.	and documents or that such erasure or destruction should be within a specified documented period. Determine if CSP has established policies that require the CSP to specifically destroy temporary files (e.g. cookies) and documents and also such erasure or destruction should be within a specified documented period. Also determine, if corresponding hardening guidelines have been established and applied to the applications.			
A7.1	Disclosure of subcontracted PII processing	MTCS Clauses 5, 9 and Annex A do not explicitly require the CSPs to disclose the use of subcontractors to its cloud service customers before their use. Determine if CSP has disclosed the use of sub-contractors to cloud service customers and whether the cloud service customers have acknowledged this disclosure.		√		

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
A9.2	Retention of security policies and guidelines	MTCS Clauses are generic and do not explicitly require copies of the obsolete policies to be retained for a period upon replacement, Determine if CSP has established policies that require the retention of copies of obsolete policies for a time period upon replacement.		√		
A9.3	PII return, transfer and disposal	MTCS Clauses 12.4, 12.11, 12.6.3, 12.8.2, 18.2 do not explicitly state that the CSP has to make the disposition of PII policy available to its cloud service customers. Determine if CSP has propagated the disposition of PII policy to cloud service customers. Also determine if CSP established a mechanism to propagate the PII policy.	MTCS Clauses 12.4, 12.11, 12.6.3, 12.6.4, 12.8.2, 18.2 do not explicitly state that the CSP has to make the disposition of PII policy available to its cloud service customers. Determine if CSP has propagated the disposition of PII policy to cloud service customers. Also determine if CSP established a mechanism to propagate the PII policy.	√	√	√
A10.1	Confidentiality Agreements	MTCS Clause 7 is not explicit about the requirement for employees or third parties being subjected to a confidentiality obligation. Determine if CSP has subjected the employees or third parties to a confidentiality obligation and they have acknowledged by signing the form.		√		√

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
A10.2	Restriction on hard copy material	MTCS Clauses 12.4, 12.5 and 12.8 do not explicitly require the CSP to have restrictions on the creation of hardcopy materials displaying PII. Determine if CSP has enhanced the Document Control Policy to include restrictions on the creation of hardcopy materials displaying PII. Also determine if the corresponding processes such as Document Information Control Procedure, Distribution lists, etc. have been enhanced to provision for such activities as control points to apply such restrictions.		√		√
A10.3	Log of data restoration	MTCS Clause 13 does not explicitly require the CSP to have a procedure or log of data restoration efforts. Determine if CSP has established the procedure for, or log of, data restoration efforts. The procedure may also consists of regular reviews being conducted to check whether logs of data restoration efforts are maintained up-to-date.		√		√
A10.9	Records of authorized users	MTCS Clause 23 does not explicitly requires for user records or profiles to be kept up-to- date. Determine if CSP has established the relevant policies to ensure users provide the latest personal information so that user records or profiles are kept up-to-date. Also determine, if corresponding processes, such as planned access reviews, have been established, to check whether user records are maintained up-to-date.		√		√
A10.10	User ID Management	MTCS Clause 23 does not explicitly state that de-activated or expired user IDs are not to be granted to other individuals.		√		

ISO 27018 Clause number	Clause title	Audit Guidance		Organisational Control	Technical Control/Visual Control Review	Effective Review
		MTCS Level 2	MTCS Level 3			
		Determine if CSP has established policies on User-ID Management, to disallow the granting of de-activated and expired user-IDs to other individuals.				
A10.11	Contract measures	MTCS Clause 10.1 does not explicitly state the following requirements. (i) requirement for the CSP to have a contract with the cloud service customer, or to ensure that the contract includes minimum technical and organisation measures to ensure that the CSP has security measures are in place and ensure that data is not processed for any purpose independent of the instructions of the customer; or (ii) Restriction against the CSP unilaterally reducing its security measures. Determine if CSP has been explicit in contractual terms with the cloud service customer to ensure that the minimum technical and organisational measures to ensure the CSP has security measures in-place and data is not processed against the instructions of the customer. Also determine if policies detail the restriction of CSP unilaterally reducing its security measures.		√		