INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Multi-Tiered Cloud Security Standard for Singapore (MTCS SS584:2015) Implementation Guidelines 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 Implementation Guidelines Report is for general information purposes only. The Implementation Guidelines Report is provided "AS IS" without any express or implied warranty of any kind. Whilst the Working Group (defined above), 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 Guidelines Report. The Working Group and IDA are entitled to add, delete or change any information in the Implementation Guidelines 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 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 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 (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 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 Implementation Guidelines Report is the second report in the set of three (3) documents to support the harmonization between MTCS SS 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 SS and the ISO 27018 Standard. The information provided in this document aims to assist entities that are MTCS SS certified to adopt the ISO 27018 Standard. CSPs that are MTCS SS certified will have to comply with the requirements stated in ISO 27018 Standard that are not fully covered in MTCS SS.		The purpose of the Implementation Guideline Report is to assist CSPs that are MTCS SS 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 SS. 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 SS audit overlaps with scope of the ISO 27001 audit.

3. Intended Audience

This Implementation Guidelines 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 SS.

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 – Implementation Guidelines

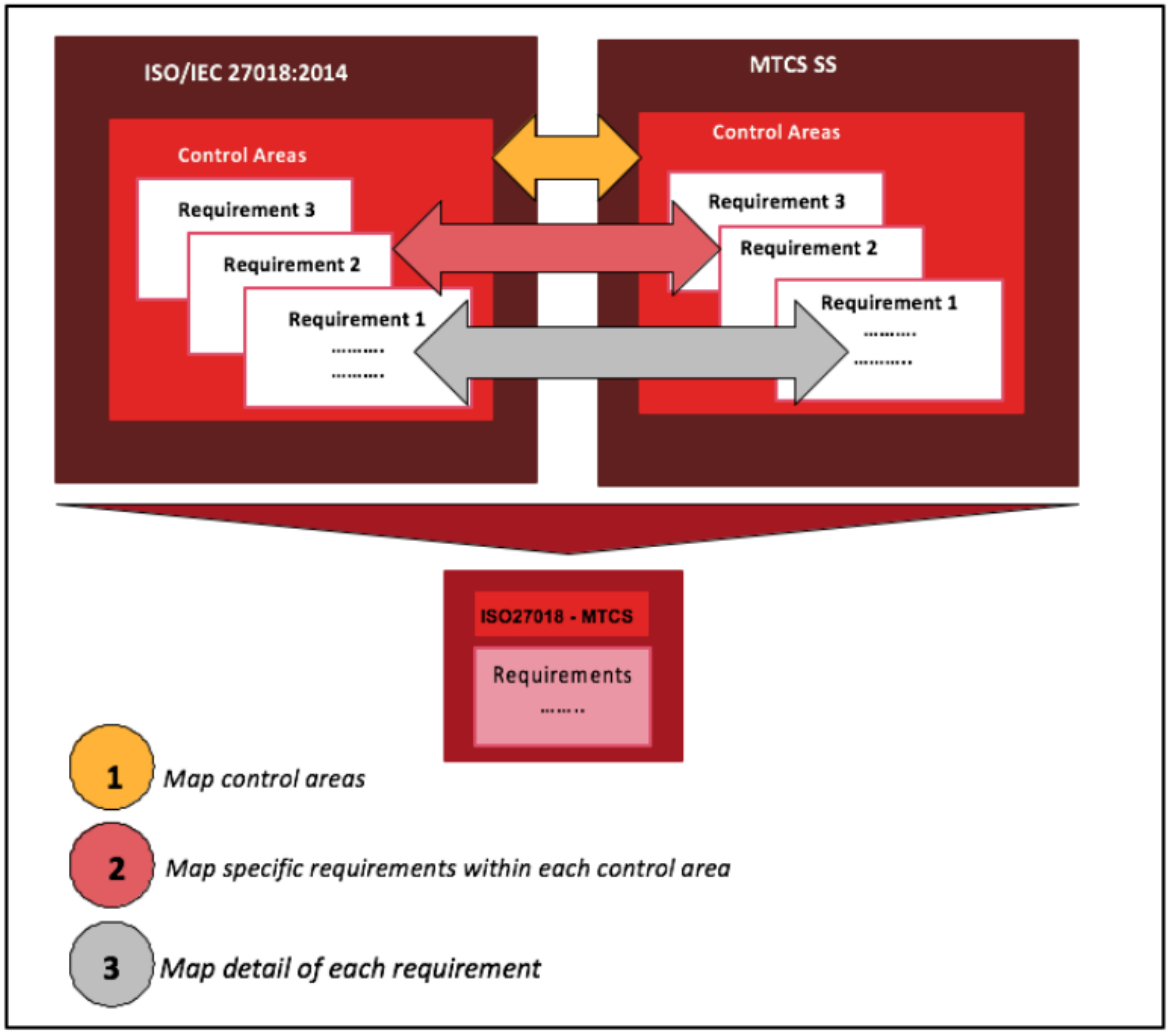
5. Terms and Definitions

All terms used within this report are derived from ISO 27018 and MTCS SS. 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 SS 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 SS 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 SS are shown in table below, were considered for mapping between ISO 27018 and MTCS SS.

However, for completeness of mapping to other clauses, please refer to the Gaps Analysis Report on cross-certification from MTCS SS 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. Implementation guidelines

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

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

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
A1.1	Obligation to cooperate with rights of PII principals	While ISO 27018 states that the public cloud PII processor 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, MTCS has no matching clause(s) to satisfy this. CSP would need to establish policies on accessing, correcting and/or erasing PII in cloud systems based on PII principals' rights and also establish the corresponding processes (e.g. access control) to provision for such activities		New Gap was found when mapping MTCS clauses to ISO 27018 Clause A1.1
A2.1	Purpose Limitation	While ISO 27018 states that PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer, MTCS has no matching clause(s) to satisfy this. CSP would need to establish policies to prevent the misuse of to-be-processed PII, resulting from deviation from the stated purpose in the cloud service customer's contract. CSP would also need to be explicit in contractual terms with the cloud service customer to ensure that there is no deviation from the stated purpose with regards to the to-be-processed PII.		New Gap was found when mapping MTCS clauses to ISO 27018 Clause A2.1
A2.2	No commercial use	While ISO 27018 states that PII processed under contract should not be used by the public cloud PII processor for marketing and advertising without consent, MTCS has no matching clause(s) to satisfy this. CSP would need to establish policies to protect the PII being processed or misused for non-consensual marketing and advertising. CSP would also need to be explicit in contractual		New Gap was found when mapping MTCS clauses to ISO 27018 Clause A2.2

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
		terms with the cloud service customer to ensure that PII would not be used for marketing and advertising without consent.		
A5.1	Disclosure notification	While ISO 27018 states 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, MTCS has no matching clause(s) to satisfy this. CSP would need to establish policies on the handling of legally binding requests with regards to the disclosure of PII and be explicit in contractual terms with the cloud service customer about disclosure notification.		New Gap was found when mapping MTCS clauses to ISO 27018 Clause A5.1

Table 1: The following requirements in ISO 27018 are partially in MTCS SS

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
5.1.1	Policies for Information Security	While ISO 27018 Clause 5.1.1 calls for CSP's Contractual agreements to clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and cloud service customer, MTCS Clauses 9.2.2(a) and 9.3.3(a) only state that roles and responsibilities of third party service providers must be documented in third party agreement. CSP should identify and document in Contractual agreements the roles and responsibilities of the public cloud PII processor, cloud service customer as well as its sub-contractor.		Partial Gap was found when mapping MTCS Clause 9.2.2, 9.3.3 and 10.1.2 to ISO 27018 Clause 5.1.1.
6.1.1	Information Security Roles and Responsibilities	While ISO 27018 Clause 6.1.1 states that public cloud PII processor should designate a contact point for Cloud Service Customer with regards to processing of PII under the contract, MTCS Clauses 6.7.1 requires a designation of an Information Security Liaison to maintain points of contacts with authorities for compliance to legislative, regulatory and contractual agreements and MTCS Clause 6.7.3(a) mentions that ISL personnel should be available for contact by Cloud Users. However, it is unclear if the ISL's responsibilities include attending to issues with regards to the processing of PII. CSP should identify and document the roles and responsibilities of the contact point designate if it is not to be clearly included in ISL personnel's roles, with regards to the processing of PII, for the Cloud Service Customer.		Partial Gap was found when mapping MTCS Clause 6.7.1 and 6.7.3(a) to ISO 27018 Clause 6.1.1.
10.1.1	Policy on the use of cryptographic controls	While ISO 27018 Clause 10.1 states that public cloud PII processor 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, MTCS Clauses 17.1.2, 17.2.2, 17.3.2, 17.3.3, 17.4.2 only mention about the usage of cryptography CSP to protect PII.		Partial Gap was found when mapping MTCS Clauses 17.1.2, 17.2.2, 17.3.2, 17.3.3 and 17.4.2 to ISO 27018 Clause 10.1.1.

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
		CSP would need to establish policies that detail the circumstances 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. CSP should also establish a mechanism to disseminate this policy to the cloud service customer.		
11.2.7	Secure disposal or re-use of equipment	While ISO 27018 Clause 11.2.7 states that for secure disposal or equipment re-use, storage media should be treated as though it contains PII, MTCS Clauses 12.8.2 and 12.9.3 only mention about secure disposal of Media (MTCS Level 1) and the entire Cloud Environment (MTCS Level 2 and above) and not about the situation about the re-use of equipment. ISO 27002 ISMS COP, Clause 11.2.7 suggests that equipment should be verified to ensure whether or not storage media is present before re-use. It is also suggested that information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function before equipment re-use. In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is re-deployed provided encryption process is sufficiently strong and covers the entire disk, encryption keys are long enough to resist brute force attacks and the encryption keys are themselves kept confidential. Overwriting tools should also be reviewed to make sure they are applicable to the technology of the storage media. CSP would need to establish policies to enforce all storage media to assume to contain PII to go through secure disk erasure prior to re-use. CSP should also establish the corresponding processes such as equipment re-use procedure etc., to provision for such activities.		Partial Gap was found when mapping MTCS Clauses 12.8.2 and 12.9.3 to ISO 27018 Clause 11.2.7. Guidelines for implementation could be found in ISO 27002 ISMS COP Clause 11.2.7.
12.1.4	Separation of development, testing and	While ISO 27018 Clause 12.1.4 requires a risk assessment be undertaken for the use of PII for testing purposes that cannot be avoided, MTCS Clauses 16.3.2 (MTCS Level 1) and 16.3.3 (MTCS Level 2 and above) is generic and prohibits the use of production		Partial Gap was found when mapping MTCS Clauses

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
	operation environments	data for testing/development unless certain safeguards are introduced. The kind of safeguards implied are also not clear. By default, all PII in the testing system should be masked, and any usage of non-masked data would have been discouraged in the first place. However, there are certain instances where machines like mainframes which are too expensive to have another server just for separate development are used. The restriction would be unclear in this case. CSP would need to perform risk assessment before using PII for testing purposes if such testing cannot be avoided.		16.3.2 and 16.3.3 to ISO 27018 Clause 12.1.4.
12.3.1	Information Backup	Though ISO 27018 Clause 12.3.1 explicitly state that CSP should (i) create multiple copies of data in physically and/or diverse locations, (ii) have a specific, documented period within which data should be restored, or (iii) review the backup procedures at a specific documented frequency, MTCS Clause 12.7.2 mentions about establishing and implementing backup procedures and scope of recovery, and to determine the frequency of testing and the access and storage locations of the backups (MTCS Level 1 and above) and MTCS Clause 12.9.3 also requires CSPs to verify the deletion of backup data (MTCS Level 2 and above). ISO 27002 ISMS COP Clause 12.3.1 states that accurate and complete records of backup copies and restoration procedures should be produced; backups should be stored in remote locations at a sufficient distance to escape any damage from a disaster at the main site; backup media should be regularly tested and combined with restoration testing procedures and checked against the restoration time required. CSP would need to enhance the backup and restoration process to include how 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.		Partial Gap was found when mapping MTCS Clauses 12.7.2 and 12.9.3 to ISO 27018 Clause 12.3.1. Guidelines for implementation could be found in ISO 27002 ISMS COP Clause 12.3.1.

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
13.2.1	Information transfer policies and procedures	Although MTCS Clauses 12.4 and 12.5 generically cover data labelling/handling and data protection (MTCS Level 1 and above), ISO 27018 explicitly states the requirement for incoming/outgoing physical media containing PII to be recorded (or the details required under ISO 27018). CSP would need to enhance policies on Asset Management to add in the requirement that incoming/outgoing physical media containing PII is to be recorded. CSP should also enhance the corresponding processes such as Asset Movement process etc., to provision for such activities.		Partial Gap was found when mapping MTCS Clauses 12.4 and 12.5 to ISO 27018 Clause 13.2.1.
16.1.1	Responsibilities and procedures for security incidents	While ISO 27018 explicitly requires a review/examination/analysis of security incidents to determine if a data breach involving PII has occurred, MTCS Clause 11 only requires CSPs to implement, maintain and periodically test incident response plans and procedures (MTCS Level 1 and above) . CSP would need to enhance the information security incident management process by having additional steps to ascertain if a data breach of PII has occurred and the corresponding follow-up to manage such incidents.		Partial Gap was found when mapping MTCS Clauses 11 to ISO 27018 Clause 16.1.1.
18.2.1	Independent Review of Information Security	While ISO 27018 explicitly requires the CSP to make available independent evidence of the CSP's implementation and operation of information security in accordance with the CSP's policy and procedures, MTCS Clause 10.2.2 requires the CSP to have independent reviews and assessments performed for policies and standards that have bearing on the relevant cloud service (MTCS Level 1 and above). ISO 27002 Clause 18.2.1 states that results of the independent review should be recorded and reported to the management who initiated the review. However, there is no indication on allowing independent evidence to be available the CSP Customers. CSP would need to make available to cloud service customers, independent evidence of the implementation and operation of information security. CSP should also establish a mechanism to make the independent evidence available to customers.		Partial Gap was found when mapping MTCS Clause 10.2.2 to ISO 27018 Clause 18.2.1.

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
A4.1	Erase Temporary Files	While ISO 27018 requires the CSP to specifically erase or destroy temporary files and documents or that such erasure or destruction should be within a specified, documented period, MTCS Clause 12.6.3 require CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS Level 2 and above), Additionally, MTCS Clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS Level 1 and above). CSP would need to establish 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. CSP should also establish the corresponding hardening guidelines to be applied to the applications.	While ISO 27018 requires the CSP to specifically erase or destroy temporary files and documents or that such erasure or destruction should be within a specified, documented period, MTCS Clauses 12.6.3 and 12.6.4 require CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS Level 2 and above), and to provide mechanisms for cloud users to remove or destroy all data (including backups) in the event of contract termination either on expiry or prematurely (MTCS Level 3 and above). Additionally, MTCS Clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS Level 1 and above). CSP would need to establish 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. CSP should also establish the corresponding hardening guidelines to be applied to the applications	Partial Gap was found when mapping MTCS Clauses 12.6.3, 12.6.4 and 12.8.2, to ISO 27018 Clause A4.1.
A7.1	Disclosure of subcontracted PII processing	While ISO 27018 explicitly requires the CSPs to disclose the use of sub-contractors to its cloud service customers before their use, MTCS Clause 9 requires CSPs to have in place an effective control framework over its third-party service providers (MTCS Level 1 and above). Additionally, under MTCS Clause 5 and Annex A, the CSP can, but is not		Partial Gap was found when mapping MTCS Clauses 5 and 9, to ISO 27018 Clause A7.1.

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
		required to, indicate whether consent from the user is required before sub-contractors are used. CSP should disclose the use of sub-contractors to cloud service customers and have them acknowledged.		
A9.2	Retention of security policies and guidelines	While ISO 27018 explicitly requires copies of the policies to be retained for a period upon replacement, MTCS sets out in a lot of detail what policies must be in place and what must be in these policies. CSP would need to establish policies that require the retention of copies of obsolete policies for a time period upon replacement.		Partial Gap was found when mapping MTCS requirements to ISO 27018 Clause A9.2.
A9.3	PII return, transfer and disposal	While ISO 27018 explicitly requires the CSP to make the disposition of PII policy available to its cloud service customers, MTCS is more generic and has all necessary controls for data handling (Clauses 12.4, 12.11, 18.2) including Clause 12.6.3 requiring CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS Level 2 and above). Additionally, MTCS Clause 12.8.2 requires CSPs to ensure that media that is no longer required is securely wiped or disposed of (MTCS Level 1 and above).	While ISO 27018 explicitly requires the CSP to make the disposition of PII policy available to its cloud service customers, MTCS is more generic and has all necessary controls for data handling (Clauses 12.4, 12.11, 18.2) including Clauses 12.6.3 and 12.6.4 requiring CSPs to have secure deletion or removal procedures when data is no longer needed (MTCS Level 2 and above), and to provide mechanisms for cloud users to remove or destroy all data (including backups) in the event of contract termination either on expiry or prematurely (MTCS Level 3 and above). Additionally, MTCS Clause 12.8.2 requires CSPs to ensure that media that is	Partial Gap was found when mapping MTCS Clauses 12.4, 12.11, 18.2, 12.6.3, 12.6.4 and 12.8.2 to ISO 27018 Clause A9.3.

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
		CSP should propagate the disposition of PII policy to cloud service customers. CSP should also establish a mechanism to propagate the PII policy.	no longer required is securely wiped or disposed of (MTCS Level 1 and above). CSP should propagate the disposition of PII policy to cloud service customers. CSP should also establish a mechanism to propagate the PII policy.	
A10.1	Confidentiality Agreements	While ISO 27018 specifically requires the employees or third parties to be subject to a confidentiality obligation, MTCS (Clause 7) is more generic and requires CSPs to have signed contracts with their employees and relevant third parties covering compliance with the CSPs responsibilities for information security, CSP should subject the employees or third parties to a confidentiality obligation and have them acknowledge by signing the form.		Partial Gap was found when mapping MTCS Clause 7 to ISO 27018 Clause A10.1.
A10.2	Restriction on hard copy material	While ISO 27018 specifically requires the CSP to have restrictions on the creation of hardcopy materials displaying PII, MTCS is more generic and Clauses 12.4 and 12.5 cover data labelling/handling and data protection (MTCS Level 1 and above), and MTCS Clause 12.8 covers the secure destruction of hardcopy materials. CSP would need to enhance the Document Control Policy to include restrictions on the creation of hardcopy materials displaying PII. CSP should also enhance the corresponding processes such as Document Information Control Procedure, Distribution lists etc.to provision for such activities as control points to apply such restrictions.		Partial Gap was found when mapping MTCS Clauses 12.4, 12.5, 12.8 to ISO 27018 Clause A10.2.
A10.3	Log of data restoration	While ISO 27018 explicitly requires the CSP to have a procedure for, or log of, data restoration efforts, MTCS (Clause 13) requires CSPs to track and monitor all access to network resources and system components. CSP should also establish the procedure or log of data restoration efforts. The procedure should also consist of regular reviews being conducted to check whether logs of data restoration efforts are maintained up-to-date.		Partial Gap was found when mapping MTCS Clause 13 to ISO 27018 Clause A10.3.

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
A10.9	Records of authorized users	While ISO 27018 explicitly requires for user records or profiles to be kept up-to-date, MTCS (Clause 23) is generic and requires the CSP to establish a formal user registration process to grant, modify and restrict user access to the cloud services (MTCS Level 1 and above). CSP would need to establish the relevant policies to ensure users provide the latest personal information so that user records or profiles are kept up-to-date. CSP should also establish the corresponding processes, such as planned access reviews, to check whether user records are maintained up-to-date.		Partial Gap was found when mapping MTCS Clause 23 to ISO 27018 Clause A10.9.
A10.10	User ID Management	While ISO 27018 explicitly states that de-activated or expired user IDs are not to be granted to other individuals, MTCS (Clause 23) is generic and requires the CSP to establish a formal user registration process to grant, modify and restrict user access to the cloud services (MTCS Level 1 and above). ISO 27002 ISMS COP Clause 9.1.1 is more generic and suggests that control should comprise of asset owners determining appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks. The policy should also take into account the security requirements of business applications, relevant legislation and contractual obligations regarding limitations of access to data or services. ISO 27002 ISMS COP Clause 9.2.1 also suggests that redundant user-ids should not be issued to others. CSP would need to establish policies on User-ID Management to disallow the granting of de-activated and expired user-IDs to other individuals.		Partial Gap was found when mapping MTCS Clause 23 to ISO 27018 Clause A10.9. Guidelines for implementation could be found in ISO 27002 ISMS COP Clauses 9.1.1 and 9.2.1.
A10.11	Contract measures	While ISO 27018 explicitly states the following are required: (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		Partial Gap was found when mapping MTCS Clause 10.1 to ISO 27018 Clause A10.11. Guidelines for

ISO 27018 Clause number	Clause title	Implementation Guidance		Additional information on gap identified
		MTCS Level 2	MTCS Level 3	
		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. MTCS is generic and Cause 10.1 requires CSPs to identify, create and maintain documentation pertaining to applicable statutory requirements (based on applicable laws where CSP's data centres are located), regulatory requirements and contractual requirements (including data protection, privacy of personal information and intellectual property rights) (MTCS Level 1 and above). ISO 27002 ISMS COP Clause 18.1.1 is generic and states that all relevant legislative statutory, contractual requirements and the organisation's approach to meet these requirements should be explicitly identified, documented and kept up-to-date for each information system and the organisation. CSP would need to be 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. Policies should also detail the restriction of CSP unilaterally reducing its security measures.		implementation could be found in ISO 27002 ISMS COP Clause 18.1.1.