CSA CYBERSECURITY CERTIFICATION

Cyber Essentials mark

Date of Publication: 03-2025 (Second edition, preview copy)

A publication by

CSA SINGAPORE

SG CYBER SAFE | CYBER ESSENTIALS

About the Cyber Security Agency of Singapore (CSA)

Established in 2015, CSA seeks to keep Singapore's cyberspace safe and secure to underpin our National Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cybersecurity awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

For more news and information, please visit www.csa.gov.sg

Contents

Page

1 Introduction 3
2 Scope 3
3 Terms and definitions 3
4 Cyber Essentials mark 5
5 References 9

Annexes

A Cyber Essentials mark — Requirements and recommendations 11

Tables

1 Security measures for Cyber Essentials mark 5
2 Example of cybersecurity requirements and/or recommendations for different digital technology environments 8

1 Introduction

The digital landscape is evolving at an unprecedented rate and offers vast and diverse opportunities for all. However, this increasingly digital way of life also increases organisational and individual exposure to cyber risks. Cybersecurity incidents can impact finances and reputation, and potentially shake consumer trust. These effects may influence business investments and overall confidence in the digital economy. Building organisations' confidence in managing cyber risks is therefore essential to enable them to harness the opportunities presented by digitalisation.

This Singapore Standard outlines tiered cybersecurity standards designed to support the cybersecurity needs of a diverse range of organisations. A framework has been developed to guide organisations in their journey towards implementing effective cybersecurity measures.

2 Scope

Organisations differ in terms of their business nature, size (which may be measured by parameters such as capital turnover or employee count), and the extent of digitalisation within their operations. These factors directly influence their cybersecurity risk profiles. This standard adopts a tiered approach to address these diverse business profiles and needs as follows:

– The Cyber Essentials mark focuses on baseline controls to protect organisations against the most common cyberattacks; and

– The Cyber Trust mark takes emphasises a risk-based approach, enabling organisations to implement appropriate cybersecurity preparedness measures with their specific cybersecurity risk profiles.

Collectively, the Cyber Essentials mark and Cyber Trust mark provide a cybersecurity risk management framework for organisations.

The cybersecurity risk management framework outlined in this standard encompasses classical cybersecurity concepts[1], cloud security, operational technology (OT) security and artificial intelligence (AI) security. This is intended to reflect how cybersecurity is not static, but a dynamic field that constantly evolves as organisations adopt[2] and utilise technology with increasing intensity[3].

This document elaborates further on the Cyber Essentials mark.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Business-critical data

Data within the organisation such as product, staff and financial information, which is vital to its operations. Loss or exposure of such data can have significant detrimental impacts, including potential financial losses and legal issues.

3.2 Certification body

[1] Typically refers to the measures that secure and protect information technology (IT) assets.
[2] Refers to percentage of organisations adopting at least 1 digital technology in Singapore Digital Economy 2023 report published by Infocomm Media Development Authority (IMDA) and Lee Kuan Yew School of Public Policy.
[3] Refers to average number of digital technologies adopted per organisation in Singapore Digital Economy 2023 report published by IMDA and Lee Kuan Yew School of Public Policy.

An organisation that has been accredited to conduct conformity assessments and issue certificates of compliance that are recognised by authorities.

3.3 Cloud service provider (CSP)

A third-party organisation that provides on-demand and scalable computing resources, such as computing power, data storage, or application services. Common cloud-based service models include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS).

3.4 Cloud shared responsibility model

A security framework that defines the shared security responsibilities between a cloud provider and its consumers.

3.5 Cyber hygiene

The practices and procedures necessary to maintain and protect an organisation's systems from threats by adopting fundamental cyber health and security postures. These measures should be commensurate with the organisation's business activities and associated risks.

3.6 End-user organisations

The organisations that consume goods or services from their providers.

3.7 Operational technology (OT)

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause direct changes through the monitoring and/or control of devices, processes, and events[4].

3.8 Passphrase

Typically, a longer-form password that uses a combination of random words, rather than solely relying on characters.

3.9 Shadow AI

The unsanctioned or adhoc use of AI tools or services by employees without the approval or oversight of the IT department.

3.10 Trust mark

A visible label or indicator of the good practices that an organisation has implemented.

3.11 Use of "shall", "should", "may" and "can"

In this standard, the following verbal forms are used:

- "shall" indicates that the requirement is strictly to be followed in order to conform to the standard and from which no deviation is permitted.
- "should" indicates a recommendation;
- "may" indicates a permission;

[4] In the context of Internet of Things (IoT) devices, whether or not they fall within "operational technology" is dependent on the deployment context of the device.

– “can” indicates a possibility or a capacity.

4 Cyber Essentials mark

4.1 Concepts and principles

The Cyber Essentials mark is designed for organisations with limited IT and/or cybersecurity expertise and resources dedicated to protecting IT assets and personnel.

The primary objective of the Cyber Essentials mark is to empower resource-constrained organisations to prioritise essential cybersecurity measures, thus safeguarding them against common cyberattacks. The Pareto principle, also known as the 80/20 rule, serves as a relevant guiding principle.

To simplify implementation for organisations embarking on their digitalisation and/or cybersecurity journey, the Cyber Essentials mark helps prioritise essential cybersecurity measures to protect against common, non-targeted attacks. Beyond classical cybersecurity, the Cyber Essentials mark also provides protection when organisations use digital technologies such as cloud, OT and AI.

The Cyber Essentials mark also serves as a badge of recognition for organisations that observe good cyber hygiene practices.

Security measures for the Cyber Essentials mark are organised into five categories, listed in Table 1. Refer to Annex A for the comprehensive list of requirements and recommendations for security measures within the Cyber Essentials mark.

Table 1 – Security measures for Cyber Essentials mark

Category: Assets	
People	Equip employees with know-how to be the first line of defence
Hardware and software	Know what hardware and software the organisation has, and protect them
Data	Know what data the organisation has, where they are, and secure the data
Category: Secure/Protect	
Virus and malware protection	Protect the organisation from malicious software like viruses and malware
Access control	Control access to the organisation’s data and services
Secure configuration	Use secure settings for the organisation’s hardware and software
Category: Update	
Software updates	Update software on devices and systems
Category: Backup	
Back up essential data	Back up the organisation’s essential data and store them separately and securely[5]
Category: Respond	
Incident response	Be ready to detect, respond to, and recover from cybersecurity incidents

[5] Not connected to the operational network

4.2 Organisational profile

An organisation's cybersecurity posture is influenced by various factors and varies significantly across organisations.

The Cyber Essentials mark is specifically targeted at resource-constrained organisations with limited IT and/or cybersecurity expertise and resources. In terms of cloud usage, these organisations typically subscribe to the SaaS cloud service model or they adopt cloud services. If these organisations utilise AI, they are generally not involved in developing or training their own AI models, but could be consuming AI services or tools from providers. Providers of IT, cloud, OT or AI products and/or services may also seek to attain the Cyber Essentials mark, based on an appropriate scope of certification.

Organisations with higher risk profiles and/or greater resources for cybersecurity should invest in more comprehensive cybersecurity measures. Such organisations should also consider applying for the trust mark. In terms of cloud usage, these organisations may subscribe to a range of cloud service models such as SaaS, PaaS and IaaS. If these organisations utilise AI, they may be involved in developing or training their own AI models, in addition to consuming AI services or tools from providers. Providers of IT, cloud, OT or AI products and/or services may also seek to attain the trust mark, based on an appropriate scope of certification.

4.3 Boundary of scope and statement of scope

Organisations shall establish the boundary of scope for certification and determine the assessable components of their environment for the Cyber Essentials mark certification.

The scope of assessment and certification can encompass the entire organisation's IT and/or OT infrastructure, or a subset, such as a specific business unit, process or location. Typically, the scope includes critical or important components for the organisation's core business. However, organisations are encouraged to include the entire IT and/or OT infrastructure within the scope of assessment and certification, where feasible, to achieve optimal protection.

The current boundary of scope shall be clearly defined, including as follows:

- The business service(s) within scope;
- The business unit(s) involved;
- The network boundary;
- The devices and/or systems within the scope;
- The software and/or services within the scope; and
- The physical location(s).

The scope of assessment and certification shall be mutually agreed upon by the organisation applying for certification and the certification body before the assessment commences. The scope of assessment and certification shall be documented and include the following:

- The organisation chart depicting the business unit(s) within the scope;
- The context of the organisation's business;
- A system and network diagram;
- An inventory listing of devices and/or systems;
- An inventory listing of software and/or services;
- Locations where the organisation operates or carries out services that are to be included within the scope of certification; and
- The Cyber Essentials mark self-assessment performed by the organisation.

Cyber Essentials mark requirements shall apply to all devices[6], systems[7] and software within this boundary of scope.

The organisation applying for certification shall also define the statement of scope used to describe the scope of certification.

When developing the statement of scope, the organisation may consider the following guiding principles:

a) Describe a critical or important aspect of the organisation's core business, e.g., "Provision of software development services in a SaaS platform" for a software development company;

b) Describe a specific subset of the organisation's core business, e.g., "Management and operations supporting the provision of software development services in a SaaS platform";

c) If the organisation operates in multiple locations, the statement of scope can also reference to the locations included within the scope; and

d) The organisation may consider a phased approach, initially starting with a smaller or narrower scope and gradually expanding the scope of certification over time.

The statement of scope shall include at least one or more of the following:

a) Classical cybersecurity;
b) Cloud security;
c) OT security; and/or
d) AI security.

A complete statement of scope shall include a description of the scope of certification and the relevant cybersecurity pillar, e,g.,

> "Product development, support and operations for [SaaS product]
> Cybersecurity pillar: Classical cybersecurity, cloud security"

As the key principles of cybersecurity are generally applicable across digital technologies like cloud, OT[8] and AI, the requirements and recommendations articulated under classical cybersecurity also apply to cloud, OT and AI security. If cloud, OT or AI security are included within the scope of certification, the cloud-, OT- or AI-specific clauses that contextualise the classical cybersecurity clauses within that digital technology environment are explicitly indicated. Where no cloud-, OT- or AI-specific clause is indicated and a "#" symbol is used, the relevant classical cybersecurity statement is also applicable in the context of that digital technology environment (see example in Table 2).

Table 2 – Example of cybersecurity requirements and/or recommendations for different digital technology environments

[6] For organisations that implement bring your own device (BYOD), where employees use their own personal mobile devices for company tasks to access the organisation's data or services, the scope of assessment and certification include such devices.
[7] For organisations that adopt cloud-based software, the scope of assessment and certification include such cloud-based services.
[8] Classical cybersecurity is typically guided by confidentiality, integrity and availability in that order; in the OT environment, the priority sequence is shifted to consider safety, availability, integrity and confidentiality.

Category	Description				Implementation status *(Yes, No)*	Remarks
	Classical cyber-security	**Cloud security**	**OT security**	**AI security**		
Assets	*Description*	*Cloud-specific description, e.g. asset inventory of cloud workloads*	*OT-specific description, e.g. asset inventory of OT assets*	*AI-specific description, e.g. asset inventory of AI services and tools*		
Secure/Protect	*Description*	*Cloud-specific description, e.g. based on cloud shared responsibility model*	*OT-specific description, e.g., use of passive scanning*	#		
Update	*Description*	#	*OT-specific description, e.g. prioritise updates for OT assets*	#		
Backup	*Description*	#	#	#		
Response	*Description*	*Cloud-specific description, e.g., include cloud-specific incidents*	*OT-specific description, e.g., include OT-specific incidents*	*AI-specific description, e.g., include AI-specific incidents*		

NOTE – For each row, use of "#" in the cloud, OT or AI security columns indicate that the statements under the classical cybersecurity column is also applicable.

4.4 How the organisation can secure its usage of digital technologies

As end-user organisations embark on digitalisation, their attack surface expands, and the organisation may start by implementing the classical cybersecurity measures in the Cyber Essentials mark to protect itself. Over time, the technology intensity[9] of organisations is expected to increase as they undergo digital transformation. As the end-user organisation adopts new technologies, such as cloud or AI, the organisation may expand its scope of certification to include other areas such as cloud security, or AI security, respectively. For organisations in industrial sectors, digital transformation may lead to a convergence of their IT and OT environments. The organisation may expand its scope of certification from classical cybersecurity, which is applicable to its IT systems, to also include OT security, for coverage of its OT systems.

Whilst the Cyber Essentials mark is not intended for product certification, organisations that are providers of IT, cloud, OT or AI products and/or services may seek certification for the Cyber Essentials mark. In the context of product and/or service providers, the organisation should consider including the end-to-end product development life cycle, operations and maintenance support of its products and/or services within the scope of certification.

4.5 Pre-certification preparation by the organisation

Before engaging a certification body, the organisation shall complete the guided self-assessment template required for Cyber Essentials mark certification.

[9] Refers to average number of digital technologies adopted per organisation in Singapore Digital Economy 2023 report published by IMDA and Lee Kuan Yew School of Public Policy.

This template consists of a list of requirements and recommendations that the organisation shall assess and indicate if these have been implemented within the organisation.

4.6 Independent assessment by certification body

Following the completion of its self-assessment, the organisation shall approach any of the certification bodies appointed by the relevant authority for independent assessment and issuance of the Cyber Essentials mark certification.

NOTE – in Singapore, certification bodies for cybersecurity certification of organisations are appointed by the Cyber Security Agency of Singapore (CSA).

When assessors from the organisation's selected certification body evaluate the organisation's application for certification, the assessors may apply professional judgement based on the business context of the organisation.

Assessors may inspect of documents and other artefacts to evaluate the relevant documentation and design of the cybersecurity measures implemented within the organisation.

For the organisation to be certified for the Cyber Essentials mark, it shall meet all requirements.

4.7 Certification life cycle

Once the Cyber Essentials mark certification has been issued to an organisation, the certification shall remain valid for a period of two years.

After the two-year certification period, the organisation may choose to re-apply for the Cyber Essentials mark. Alternatively, the organisation may also consider seeking Cyber Trust mark certification if its risk profile has changed.

NOTE: Annex A contains the comprehensive list of requirements and recommendations of security measures in the Cyber Essentials mark.

5 References

In preparing this document, reference was made to the following publications:

1. Cyber Essentials and Cyber Trust mark (2022) by Cyber Security Agency of Singapore
2. ISA/IEC 62443 series on security of industrial automation and control systems
3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements
4. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
5. ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
6. ISO/IEC 42001:2023 Information technology – Artificial intelligence – Management system
7. Baseline cyber security controls for small and medium organisations V1.2 by Canadian Centre for Cyber Security
8. CIS controls v8 by Centre for Internet Security
9. CIS controls v8 cloud companion guide by Centre for Internet Security
10. CIS password policy guide by Centre for Internet Security
11. CISA cyber resilience review (CRR) by US Department of Homeland Security (DHS) and CERT Division of CMU Software Engineering Institute
12. Cyber Essentials by UK National Cyber Security Centre (NCSC)

13. Cyber risks associated with generative artificial intelligence by Monetary Authority of Singapore (MAS)
14. Cybersecurity maturity model certification (CMMC) by US Department of Defence
15. Cybersecurity playbook for large language model (LLM) applications by Government Technology Agency (GovTech)
16. Essentials 8 by Australian Cyber Security Centre
17. Federal Financial Institutions Examination Council (FFIEC) cybersecurity assessment tool
18. Federal Risk and Authorisation Management Programme (FedRAMP) by US federal government
19. HiTrust by Health Information Trust Alliance
20. NIST cybersecurity framework (CSF) 2.0
21. Payment card industry data security standard (PCI DSS) by Visa, MasterCard, Discover Financial Services, JCB International and American Express
22. SP 800-82r3 guide to operational technology (OT) security by National institute of Standards and Technology (NIST)
23. SOC for service organisations by American Institute of Certified Public Accountants (AICPA)
24. Technology risk management guidelines (TRMG) by Monetary Authority of Singapore (MA
25. The Five ICS cybersecurity critical controls by SANS Institute

Acknowledgement is made for the use of information from the above publications.

Annex A
(normative)

Cyber Essentials mark – Requirements and recommendations

The key principles of cybersecurity are generally applicable across digital technologies like cloud, OT and AI. If cloud, OT and/or AI security are included in the scope of certification, digital technology-specific clauses that contextualise the classical cybersecurity clauses for that digital technology environment are indicated explicitly. Where there is no digital technology-specific clause indicated and a "#" symbol is used, the relevant classical cybersecurity requirement or recommendation is also applicable in the context of that digital technology environment.

For each row, use of "#" in the cloud, OT or AI security columns indicate that the statements under the classical cybersecurity column are also applicable.

A.1 Assets: People – Equip employees with know-how to be the first line of defence

A.1.1 Introduction

Employees are the first line of defence in the organisation and the weakest link in the security chain, as cyber attackers increasingly use social engineering techniques to target them for their agenda. Therefore, it is essential for all employees to be well-trained to identify these techniques, mitigate them, and report any suspected incidents promptly.

A.1.2 Applicability

All employees within the scope of assessment and certification in the organisation that have access to the organisation's IT assets and/or environment.

A.1.3 Objective

To actively instil cybersecurity awareness among employees across all levels within the organisation. In addition, encourage the cultivation of a culture of shared responsibility in cybersecurity within the organisation.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.1.4 (a)	The organisation shall establish cybersecurity awareness and data protection training for all employees to ensure they are aware of the security practices and behaviour expected of them. Organisations may achieve this through	#	As teams managing OT and IT are typically distinct and may operate independently, OT-specific security	#

	various means, e.g., provide self-learning materials for employees or engaging external training providers.		awareness training shall be provided to: – Employees that are involved in operating, securing and maintaining the OT environment; and – IT employees where IT and OT operations converge.	
A.1.4 (b)	Cyber hygiene practices and guidelines shall be developed for employees to adopt in their daily operations.	#	OT security practices and guidelines shall account for the requirements of the OT environment and be integrated with existing IT cybersecurity practices. Such practices and guidelines shall include identifying critical connectivity and assets that are required in reduced or constrained operations in the event of a cybersecurity incident.	#
A.1.4 (c)	Cyber hygiene practices and guidelines should include measures to mitigate cybersecurity incidents arising from human factors, as follows: – Be vigilant against the rise of AI-enabled social engineering and deepfake attacks; – Secure access with Multi-Factor Authentication (MFA) and strong passphrases and protect them; – Protect corporate and/or personal devices used for work, i.e., BYOD;	The cyber hygiene practices and guidelines should include cloud-specific topics as follows: – Shared responsibility in the cloud: Be aware of your responsibilities for cybersecurity as a cloud user;	The cyber hygiene practices and guidelines topics should include OT-specific topics as follows: – Operational security: Be aware of best practices for maintaining the security of the OT system; – Common risks in OT environments, including	The cyber hygiene practices and guidelines topics should include AI-specific topics as follows: – Governance of business-critical data when using public or enterprise AI tools or services: Perform data housekeeping, classify,

	– Handle and disclose business-critical data, including personal data with care; – Maintain secure work practices both on-site and remotely; and – Report all cybersecurity incidents promptly.	– Accessing the cloud: Protect your access to cloud services; – Cloud configuration settings: Review and secure default cloud service configurations; and – Data stored in the cloud: Protect data during transfer to and while stored in the cloud.	how IT-centric events can impact OT operations; – Suspicious activity in the OT environment: How to detect and flag suspicious activity for further investigation; and – OT incident response: How to respond to suspected incidents within the OT environment. The organisation should contextualise these topics for its specific OT applications.	handle and disclose data appropriately; and – Common risks associated with using AI in the organisation.
A.1.4 (d)	Where feasible, the training content should be differentiated based on employee roles as follows: – Senior management or business leaders – Developing a cybersecurity culture/mindset within the organisation or establishing a cybersecurity strategy or workplan; – Employees – The use of strong passphrases, the protection of corporate and/or personal devices used for work; and – Employees handling personal data – Ensure familiarity with topics on personal data protection, NOTE – In Singapore, the Personal Data Protection Commission offers e-learning programme for handling personal data.	The differentiation may be based on different roles involved in the use of cloud services as follows: – Senior management or business leaders – Balancing trade-offs between business and cloud security risks, including cyber resilience and dependency on major CSPs; and – Employees – Secure handling of business-critical and personal data in the cloud, as well as securing user cloud access and settings when using cloud services.	The differentiation may be based on different roles involved in OT operations as follows: – Senior management or business leaders – Balancing trade-offs between OT security risks and the extended use of legacy OT systems; – OT engineers and operators – Security of OT systems; – Physical security personnel – The use of physical access controls in the OT environment as compensating controls when OT systems do not	The differentiation may be based on different roles involved in the use of AI tools or services as follows: – Senior management or business leaders Balancing trade-offs between business and AI security risks, including over-reliance on AI and/or AI providers; and – Employees – Secure handling and disclosure of business-critical data when using public or enterprise AI services, including generative AI services.

			– support modern IT logical access control; and – Employees handling IT – Areas where IT and OT operations converge.	
A.1.4 (e)	As a best practice, such cybersecurity awareness initiatives should be conducted at least annually to refresh employee awareness.	#	#	#

A.2 Assets: Hardware and software – Know what hardware and software the organisation has and protect them

A.2.1 Introduction

Knowledge about the environment is the foundation of an effective cybersecurity strategy. Taking stock of the hardware and software in the organisation is fundamental to an effective cybersecurity strategy. This process ensures that the assets are (i) authorised to access the organisation's environment and (ii) secured properly.

A.2.2 Applicability

Hardware within the scope of assessment and certification includes the organisation's assets such as end-user devices (e.g., desktop computers, laptop computers, portable and mobile devices such as tablets and mobile phones, network devices such as firewalls and routers, and non-standard computing devices such as IoT devices and servers (e.g., email, web and application servers).

Software within the scope of assessment and certification includes business applications, online services accessed using business email, and other applications accessed locally or remotely via the devices.

A.2.3 Objective

To actively manage the hardware and software assets within the organisation's environment. Having asset visibility enables the implementation of effective monitoring and protection measures. Active asset management also ensures that only authorised assets and devices are used and that only authorised software are installed.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security

<table>
<tr>
<td>A.2.4 (a)</td>
<td>The organisation shall maintain an up-to-date asset inventory of all the hardware and software assets, including those from third-party vendors. Methods for maintaining this inventory may include the use of spreadsheets or IT asset management software to maintain the IT asset inventory. Organisations shall also include network diagrams and drawings of their environment.</td>
<td>This shall include cloud-based assets, such as:

– SaaS subscriptions;
– other cloud service models such as IaaS and PaaS subscriptions, including cloud instances, such as software, virtual machines, containers and operating systems (OS); and
– interfaces and/or APIs to the cloud.</td>
<td>This shall cover OT assets from the Intelligent Devices Zone in Level 1 and above in the Purdue model.

The OT asset inventory shall differentiate between the critical connectivity and assets essential for reduced or constrained operations during cybersecurity incidents.</td>
<td>This shall include any usage of, or subscription to, AI tools or services, such as:

– free or public AI services; and
– enterprise AI tools

This inclusion aims to mitigate the risks associated with “shadow AI” within the organisation.</td>
</tr>
<tr>
<td>A.2.4 (b)</td>
<td>Hardware assets within the scope of certification may include servers, network devices, laptops and computers. If the scope of the certification includes hardware assets such as mobile devices and/or IoT devices, note the following:

<table>
<tr><td>Mobile devices</td><td>– Organisations should include company-issued mobile devices as part of its asset inventory, such as mobile phones or tablets.</td></tr>
<tr><td>IoT devices</td><td>– The inventory should include IoT devices used within the organisation such as closed-circuit television (CCTV) cameras, smart printers and smart televisions.</td></tr>
</table>
</td>
<td>#</td>
<td>For IoT devices, their inclusion within the OT environment depends on their deployment context, e.g., CCTVs that are used to support physical security within an OT environment shall be included in the scope.</td>
<td>#</td>
</tr>
<tr>
<td>A.2.4 (c)</td>
<td>The inventory list should contain details of the hardware assets, where available, as follows:

– Hardware name/model;
– Asset tag/serial number;</td>
<td>#</td>
<td>Additionally, the inventory list of OT hardware assets should also capture the firmware version installed in these assets.</td>
<td>#</td>
</tr>
</table>

	– Asset type; – Warranty information; – Asset location; – Network address; – Asset owner; – Asset classification; – Department; – Approval/authorisation date; – Service Level Agreements (SLAs); – End of support (EOS) date; and – Vendor contact information.			
A.2.4 (d)	The inventory list should contain details of the software assets, where available, as follows: – Software name; – Software publisher; – Software license key (including API keys); – Software version; – Business purpose; – Asset classification; – Approval/authorisation date; – Service level agreements (SLAs); – EOS date; and – Vendor contact information.	#	#	The inventory list of AI assets should additionally include: – free or public AI services; and – enterprise AI tools.
A.2.4 (e)	As a best practice, the hardware and software asset inventory list should be reviewed at least bi-annually (twice per year).	#	#	#
A.2.4 (f)	Unauthorised hardware and software assets, or those that have reached their respective EOS dates shall be removed.	#	#	#
A.2.4 (g)	In cases where continued use of EOS assets is necessary, the organisation shall assess and understand the cybersecurity risk, obtain	#	The assessment for continued active use of EOS OT assets that may not	#

	approval from senior management and monitor it until the asset is replaced.		adequately support cybersecurity shall include: – outlining the risks involved; and – the compensating controls implemented to manage the risks.	
A.2.4 (h)	An authorisation process shall be developed for onboarding new hardware and software into the organisation. Methods may include email approval from senior management, ensuring that new hardware or software originate from official or trusted sources, and performing malware scans to verify the asset's integrity. Asset whitelisting/blacklisting may also be implemented.	For cloud-based assets, e.g., for SaaS, the authorisation process may include verification of the cybersecurity posture and track record of the SaaS provider.	For OT assets, the authorisation process may include a sanitisation process, e.g., scanning new hardware and software for malicious code prior to onboarding. When introducing external devices and removable storage media, e.g., those used by the organisation's OT vendors for support and maintenance, the organisation shall do so only when necessary and only after a sanitisation process has been performed, as these devices and media may be used by vendors to support multiple customer deployments, potentially leading to "cross-infection" from other infected sites.	For AI assets, the authorisation process may include verification of the cybersecurity posture and track record of the source or provider of the AI assets, or scanning for malicious code.
A.2.4 (i)	The date of authorisation for software and hardware shall be included in the asset inventory list after obtaining the relevant	#	#	#

	approval, e.g., through email or with an approval form.			
A.2.4 (j)	Software and hardware without approval shall not be used in the organisation.	#	#	#
A.2.4 (k)	Before disposing of any hardware asset, the organisation shall ensure that all critical or confidential information is securely wiped, sanitised, or otherwise destroyed, e.g., encrypting hard disk before reformatting and overwriting it.	The organisation should review the CSP's practices for the disposal of hardware assets to ensure alignment with its requirements.	#	#
A.2.4 (l)	When disposing of hardware assets, the organisation should implement secure disposal methods, e.g., destroying the hard disks physically or engage disk shredding services.	The organisation should review the CSP's practices for the disposal of hardware assets to ensure alignment with its requirements.	#	#

A.3 Assets: Data – Know what data the organisation has, where they are and secure the data

A.3.1 Introduction

Data is the organisation's most valuable business asset. Identifying the critical data in the organisation is foundational to classifying, monitoring and protecting it, thus ensuring its security and enabling authorised access.

A.3.2 Applicability

Data within the scope of assessment and certification includes raw and unorganised facts such as numbers or text on paper, bits and bytes stored in electronic memory, system memory size, employee names, product names, addresses and costs of service.

A.3.3 Objective

To actively manage data in the organisation's environment. Having visibility of the types of data the organisation collects, processes and stores enables the implementation of effective monitoring and protection measures to prevent unauthorised access and/or disclosure.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.3.4 (a)	The organisation shall identify and maintain an inventory of business-critical data[10]. Methods may include using spreadsheets or asset inventory software. The inventory list shall contain details of the data as follows: – Description; – Data classification and/or sensitivity; – Location; and – Retention period. For organisations holding substantive personal data that could result in a breach of a significant scale, the organisation shall also document the data flow diagram for personal data.	For data stored and processed in the cloud, the organisation shall additionally include the following information in its inventory: – CSP; and – cloud service.	The inventory shall include OT-related data stored in the cloud or on vendor servers. Examples of OT-related data include: – OT-specific data – e,g., sensor data, computer-aided drafting/computer-aided manufacturing files, controller configuration files; and	The inventory shall include an indication of the data sets that are: – used as input to AI tools or services within the organisation; – generated as output from key AI tools or services within the organisation; and – the corresponding AI tools or services within the organisation that

[10] This includes confidential and/or sensitive data including personal data. Examples include data within the organisation such as product, staff and/or financial data that is vital to the organisation's operations and where exposing them can lead to potential financial losses and/or legal issues.

			– OT-specific processes – e.g., program code for ladder logic.	consume or generate these data sets.
A.3.4 (b)	The inventory list should be reviewed at least annually, or whenever there are changes to the data captured by the organisation.	#	#	#
A.3.4 (c)	The organisation shall establish a process to protect its business-critical data, e.g., password-protecting documents, encrypting emails, protecting organisational data on employee personal devices used for work (i.e., BYOD), which include personal laptops, mobile devices, and USB devices. For organisations holding substantive personal data that could result in a breach of a significant scale, the data shall be encrypted both at rest and in transit.	For the storage and protection of business-critical data in the cloud, the organisation shall assess the following: – The type of data and how it is transferred to and from the cloud; – The level of data access granted to the CSP; – The potential impact on the organisation if it loses access to its data in the cloud; and – Geolocation requirements for data storage, processing and transmission to meet client requirements, considering that cloud services may replicate data across multiple servers and locations. The organisation shall implement relevant mechanisms supported by its	Protection of data in the OT environment may require the implementation of physical and/or access controls. When applying encryption in the OT environment, the organisation may need to consider the potential impact of encryption latency on OT operations.	For the protection of data used in AI tools and services, the organisation shall perform the following: – Assess whether the sensitivity or classification of data used as input for AI tools and services could lead to negative consequences if leaked; – Review the integrity of data used as input to AI within the organisation and implement data sanitisation measures where relevant to mitigate the risk of input data manipulation influencing AI output; and – Review the integrity of data generated as output from AI within the organisation to mitigate the risk of potential

		CSPs to protect its business-critical data in the cloud, which may include: – granular controls for sharing data; – encryption of data in-transit and at rest; – support for secure protocols, e.g., transport layer; – capabilities for identifying and/or masking sensitive data; and – mechanisms for cloud users to tag sensitive data or fields.		manipulation or hallucinations.
A.3.4 (d)	Measures shall be implemented to prevent employees, third parties and contractors from disclosing or leaking confidential and/or sensitive data outside the organisation. Examples include: – disabling USB ports; and/or – including clauses regarding unauthorised disclosure of information in employment contracts and contractual agreements with third parties or contractors.	#	The organisation shall limit the use of (or use dedicated) external media and devices for connecting to OT assets (including those used by the organisation's OT vendors) to protect against the loss or theft of OT data and the introduction of malware to OT assets.	The organisation shall implement measures to control the use of data in the organisation for: – input to external or public AI tools and services, e.g., mitigate against data leakage; and – input to internal or enterprise AI tools and services, e.g., appropriate data classification across functional divisions in the organisation.

A.3.4 (e)	Before disposing of any physical media containing confidential and/or sensitive data, e.g., paper, the organisation shall ensure that the data is securely destroyed, such as by shredding the media.	#	#	#

A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware

A.4.1 Introduction

Malware poses a significant threat to organisations when hardware and software are connected to the internet. Malware is designed to attack systems, devices and steal data. It can infiltrate through various channels, including end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Moreover, malware evolves rapidly, necessitating frequent updates to detection mechanisms to maintain effective protection.

A.4.2 Applicability

Hardware within the scope of assessment and certification includes the organisation's assets such as end-user devices (e.g., desktop computers, laptops, as well as portable and mobile devices such as tablets and mobile phones), network devices (e.g., firewalls, routers), non-standard computing devices (e.g., IoT devices), and servers (e.g., email, web and application servers), including cloud-hosted systems.

Software within the scope of assessment and certification includes those installed in servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, storage solutions and virtualisation platforms.

A.4.3 Objective

To ensure adequate protection measures are in place to continuously monitor and defend against malware, as it can compromise network access and cause damage to the organisation's environment.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.4.4 (a)	Virus and malware protection solutions shall be used and installed on endpoints (e.g., laptop	The organisation shall refer to the cloud shared	The organisation shall implement measures to protect OT endpoints from	#

	computers, desktop computers, servers, virtual environments) to detect attacks.	responsibility model with its CSP. For SaaS, the organisation shall verify that the CSP has implemented virus and malware protection solutions for the cloud services. For other cloud service models where the organisation is responsible, the organisation shall implement virus and malware protection solutions on its cloud workloads.	viruses and malware, such as the following: – Virus and malware scans at entry points before endpoints connect into the OT environment; – Virus and malware protection solutions that have been tested for compatibility with the OT environment and recommended by the OT vendor; or – Compensating controls such as network-based virus and malware protection solutions or application whitelisting.	
A.4.4 (b)	Virus and malware protection solutions shall be configured to automatically scan files upon access to detect potential cyberattacks. This includes files and attachments downloaded from the internet through web browsers or email, and external sources such as from portable USB drives. Where feasible, scans should always remain active to provide constant protection.	Virus and malware protection solutions shall perform automatic scans of files ingested into the organisation's cloud service.	The organisation may perform manual scanning on OT assets during scheduled maintenance windows or downtime when automated scans disrupt OT operations. The configuration of virus and malware protection solutions shall be tested, e.g., on an offline system where feasible.	#
A.4.4 (c)	Automatic updates or configurations for virus and malware protection solutions shall be enabled to update signature files or equivalent (e.g., non-signature-based machine learning	#	The organisation may perform signature updates on OT systems during scheduled maintenance	#

<table>
<tr><td></td><td>solutions) to detect new malware. At least daily updates are recommended for optimal protection.</td><td></td><td>windows or downtime when auto-updates disrupt OT operations.</td><td></td></tr>
<tr><td>A.4.4 (d)</td><td>If the scope of certification includes mobile devices, IoT devices, or web browser/email use:

<table><tr><td>Mobile devices</td><td>– Virus and malware protection solutions should be installed and running on mobile devices.</td></tr><tr><td>IoT devices</td><td>– Virus and malware protection solutions should be integrated with IoT devices, e.g., CCTVs, smart televisions, smart printers, digital door locks.</td></tr><tr><td>Web browser / Email</td><td>– Only fully supported web browsers and email client software with security controls should be used.
– Anti-phishing and spam filtering tools should be implemented for web browsers/email clients.
– Web browsers and/or email plug-ins/extensions/add-ons that are not necessary should be disabled and/or removed.
– Web filtering should be deployed to protect the business from malicious websites, where feasible.
– Email authentication protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication</td></tr></table></td><td>#</td><td>#</td><td>#</td></tr>
</table>

	Reporting and Conformance (DMARC) should be implemented to provide email security.			
A.4.4 (e)	Firewalls shall be configured and deployed to protect the network, systems, and endpoints such as laptops, desktops, servers, and virtual environments. Depending on the organisation's network setup, the firewall functionality may be integrated with other networking devices or deployed as a standalone device. In an organisation that has a network setup, a network perimeter firewall (e.g., Domain Name System (DNS) firewall and application-level gateway firewall) shall be configured to analyse and accept only authorised network traffic and deployed. In an organisation that comprises of just endpoints connecting to the internet and/or cloud-based applications, similarly, firewalls (e.g., software firewall (host-based firewall) built-in/included in operating systems, firewall integrated with the organisation's router or wireless access point) shall be configured and deployed.	The organisation shall refer to the cloud shared responsibility model with its CSP. For SaaS, the organisation shall verify that the CSP has implemented network security measures, e.g., firewall, to protect the cloud services. For other cloud service models where the organisation is responsible, the organisation shall implement network security measures, e.g., firewall, to protect its cloud workloads.	The organisation shall: – use firewalls for segmentation between OT and IT (or corporate) networks to only allow authorised traffic to/from the IT network, e.g. segment OT assets or services that require external connections to the IT (or corporate) network; – segment the OT network, considering the OT assets that can be reduced in constrained operations during a cybersecurity incident; and – establish boundaries at each network segment to manage all ingress and egress communication traffic. Where relevant, unidirectional gateways, e.g., data diodes, may also be used to enforce unidirectional traffic.	#

A.4.4 (f)	As good practice, firewall configurations and rules should be reviewed and verified annually to protect internet-facing assets where applicable.	#	#	#
A.4.4 (g)	If the scope of certification includes mobile and/or IoT devices: Mobile devices – Firewalls should be installed and enabled on employees' mobile devices. IoT devices – Firewalls should be configured and enabled on IoT devices where possible.	#	#	#
A.4.4 (h)	The organisation shall ensure employees install and use only authorised software, and access only attachments from official or trusted sources to ensure the integrity of the software, e.g., code signing.	#	#	#
A.4.4 (i)	The organisation shall ensure employees use only trusted network connections for accessing the organisation's data or business email, e.g., mobile hotspot, personal Wi-Fi, corporate Wi-Fi and virtual private network (VPN).	#	For remote access to the OT environment, the organisation shall: – limit remote access as much as possible; and – use secured connections, e.g., VPNs and support MFA where feasible, e.g., jump host with MFA.	#
A.4.4 (j)	The organisation shall ensure employees immediately report any suspicious email or attachment to the IT team and/or senior management.	#	Given the deterministic nature of the OT environment and its predictable and repeatable network traffic, the organisation shall ensure that employees recognise	The organisation shall ensure employees report AI security concerns or unexpected AI behaviour for further investigation.

			unusual traffic patterns and report suspicious activities for further investigation.	

A.5 Secure/Protect: Access control – Control access to the organisation's data and services

A.5.1 Introduction

Active user accounts and physical access serve as entry points to an organisation's hardware and software. Restricting access to authorised users minimises the risk of data theft and hardware/software compromise.

A.5.2 Applicability

Hardware within the scope of assessment and certification includes the organisation's assets such as end-user devices (e.g., desktop computers, laptops, portable and mobile devices such as tablets and mobile phones), network devices (e.g., firewalls, routers), non-standard computing devices (e.g., IoT devices), and servers (e.g., email, web and application servers) including cloud-hosted systems.

Software within the scope of assessment and certification includes those installed on servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers and storage solutions and virtualisation platforms.

A.5.3 Objective

To ensure adequate protection measures are in place to limit access to the organisation's environment by employees and other third parties, including contractors.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.5.4 (a)	Account management shall be established to maintain and manage the inventory of accounts. Methods may include spreadsheets or exporting lists from software directory services.	The inventory shall include the organisation's access to the cloud, e.g., login accounts, APIs.	#	The inventory shall include the organisation's access to its AI tools and services, e.g. login accounts, APIs.

A.5.4 (b)	The account inventory list shall include details for user, administrator, third-party and service accounts, not limited to the following: – Name; – Username; – Department; – Role/account type; – Date of access created; and – Last logon date.	#	For OT assets that support only a limited number of accounts using shared credentials, the account inventory list shall include: – shared accounts; – associated OT assets; and – employees sharing the account. The account inventory list shall additionally include: – accounts that require time-critical, quick access in emergencies; and – the secure location (where applicable) for storing these passwords for quick intervention by OT operators in emergencies. For OT systems that do not support password recovery, the organisation shall ensure secure and reliable handling of passwords to maintain continuous operation.	#
A.5.4 (c)	The organisation shall implement an approval process (e.g., email approval or access request form) to grant and revoke access. This shall be implemented when there are personnel changes such as new hires or role changes. The following fields shall be captured:	#	As part of the approval process, the organisation shall ensure that employees with access to both OT and IT (or corporate) networks use segregated	#

	– Name; – System to access; – Department; – Role/account type; – From date; and – To date.		authentication mechanisms and/or separate credentials to prevent the use of compromised IT credentials to access the OT environment.	
A.5.4 (d)	Access shall be managed to ensure employees can access only the information and systems required for their job role.	The organisation shall implement limitations on employee access to cloud services, such as using the following: – Allow user access only from approved devices; – Set resource limit to accounts or services; and – For BYOD arrangements, limit access to key cloud services.	#	#
A.5.4 (e)	Accounts with unnecessary or expired access rights shall be disabled or removed from the system. Shared, duplicate, obsolete, dormant and inactive accounts (e.g., inactive for more than 60 days) shall be removed.	#	For OT assets that can only support limited number of accounts resulting in shared credentials, the organisation shall implement additional controls, e.g.: – role-based access, – physical access control; and – performing OT monitoring.	#
A.5.4 (f)	The administrator account shall only be created with approval from senior management and be used for administrator functions. The	#	#	#

	administrator account shall not be used for daily activities.			
A.5.4 (g)	Access shall be managed to ensure third parties or contractors can access only the information and systems required for their job role. Such access shall be removed when no longer needed.	#	For organisations relying on OT vendors for technical support and maintenance activities, the organisation shall: – limit remote access as much as possible; – use secured connections, e.g., VPNs with screen sharing software and support MFA where feasible, e.g., jump host with MFA; – implement network segmentation for more granular access management; and – secure third party access such as use of two-part passphrases, where one part is held by the OT asset owner and the other part by the third party, so that the third party does not gain access without the knowledge of the OT asset owner.	#
A.5.4 (h)	Third parties or contractors working with sensitive information shall sign a non-disclosure agreement outlining contractual actions for non-compliance.	#	#	#

A.5.4 (i)	The organisation should implement minimum cybersecurity requirements for third parties or contractors working with confidential and/or sensitive data and ensure its third parties or contractors inform the organisation of any relevant cybersecurity incidents involving these third parties or contractors. NOTE – In Singapore, Cyber Essentials is one of the certifications that help organisations implement fundamental cybersecurity measures.	The organisation should assess if its CSPs adhere to relevant industry standards. NOTE – In Singapore, Multi-Tier Cloud Security Standard (MTCS) is relevant for CSPs that offer IaaS, or Cyber Trust for CSPs that offer SaaS. The organisation should review CSP practices for the following to ensure alignment with its requirements: – SLAs for cloud service availability, and the protection of data confidentiality and integrity; and – Vulnerability assessment and penetration tests conducted by the CSPs.	#	#
A.5.4 (j)	Physical access control shall be enforced to secure the organisation's information assets and/or environment, allowing access only to authorised employees/contractors, e.g., use of cable locks for workstations, card access door locks to authenticate and authorise entry.	#	In addition to securing the organisation's physical environment, physical access control may be applied to the OT environment as compensating controls when OT systems do not support modern IT logical access control, e.g., securing OT assets in a locked cabinet or room where access is managed to prevent	#

			unauthorised access if ports cannot be logically disabled.	
A.5.4 (k)	As good practice, account reviews should be carried out at least quarterly or whenever there are changes to the account list, e.g., during onboarding and offboarding processes or organisation restructuring.	#	#	#
A.5.4 (l)	The organisation shall change all default passwords and replace them with a strong passphrase (it should be at least twelve characters, including upper case, lower case and/or special characters).	#	If default passwords cannot be changed for OT assets, the organisation shall implement compensating controls such as physical security (or isolation) or network segmentation. If strong passwords are not supported by the OT assets, the organisation shall configure passwords on such devices to the maximum password strength that can be supported. If passwords are transmitted in cleartext by the OT assets, rendering them vulnerable to interception, the organisation shall use unique passwords with encrypted and non-encrypted protocols. Where operator lock-out or delayed access to the OT assets can lead to potential safety issues and where password protection is not	#

			recommended, e.g., control consoles on critical processes, the organisation shall implement compensating controls, e.g., physical or network isolation.	
A.5.4 (m)	User accounts shall be disabled and/or locked out after multiple failed login attempts, e.g., ten failed login attempts, rate-limiting attempts[11].	#	For OT assets where disabling or locking accounts after multiple failed attempts is not supported or appropriate, the organisation may implement compensating controls such as physical access control or passive monitoring and detection.	#
A.5.4 (n)	The account password shall be changed in the event of any suspected compromise.	#	For OT assets where passwords cannot be changed, the organisation may implement compensating controls such as physical access control.	#
A.5.4 (o)	MFA shall be used for administrative access to important systems and database servers containing sensitive or business-critical data, or a substantive amount of personal data that could result in a breach of a significant scale. MFA methods include authenticator applications and one-time password (OTP) tokens.	#	For OT assets where MFA cannot be supported, the organisation may implement compensating controls such as physical security (or isolation), network segmentation or use of two-part passphrases, which require two parties to access the system.	#

[11] This means that the time the user needs to wait between attempts increases with each failed login attempt.

A.5.4 (p)	Where feasible, the organisation should implement additional measures to assist employees with secure passphrase management, e.g. trusted software to manage passphrases such as passphrase or password managers, passwordless authentication.	For organisations with a large number of cloud services, solutions should be implemented to assist employees with secure password management for multiple individual cloud services. This may include solutions such as the use of identity providers for single sign-on (SSO). If separate passwords need to be managed and maintained, the organisation should: – implement the use of secure passphrases; – ensure passphrases are not reused across multiple cloud services or corporate accounts; and – ensure passphrases are not shared across accounts.	#	#

A.6 Secure/Protect: Secure configuration – Use secure settings for the organisation's hardware and software

A.6.1 Introduction

Hardware and software are typically shipped with default settings from manufacturers, often prioritising ease of deployment and use. These unsecured default settings can be readily exploited.

A.6.2 Applicability

Hardware within the scope of assessment and certification includes the organisation's assets such as end-user devices (e.g., desktop computers, laptops, as well as portable and mobile devices such as tablets and mobile phones), network devices (e.g., firewalls, routers), non-standard computing devices (e.g., IoT devices), and servers (e.g., email, web and application servers) including cloud-hosted systems.

Software within the scope of assessment and certification includes those installed on servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, storage solutions and virtualisation platforms.

A.6.3 Objective

To ensure adequate protection measures are in place to secure the configurations and settings of hardware and software, thereby mitigating risks associated with exploits or vulnerabilities arising from default administrator passwords.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.6.4 (a)	Security configurations shall be enforced for the assets including desktop computers, servers and routers. Methods may include adopting industry recommendations and standards, running baseline security analysers and securing the system configuration, e.g. using scripts. NOTE – One of the organisations that offer security configuration guidelines is Center for Internet Security (CIS).	The organisation shall implement the secure configuration best practices and/or settings published by its CSPs, if available.	The organisation shall identify and implement secure configurations for OT assets and maintenance devices within the OT environment based on secure configuration best practices and/or settings provided by OT vendors to mitigate against common attacks. Where secure configuration is not feasible for OT assets, the	Such secure configuration best practices and/or settings shall also apply to the environment being used to deploy the organisation's AI tools or services.

			organisation shall implement compensating controls. The secure configuration shall be tested prior to implementation, e.g., by the OT vendor on an offline system. Such configuration shall also be reviewed after maintenance and software patching, as features may have been inadvertently re-enabled or new features installed.	
A.6.4 (b)	Insecure configurations and weak protocols shall be replaced or upgraded to address the associated vulnerabilities, e.g., – using hypertext transfer protocol secure (HTTPS) instead of hypertext transfer protocol (HTTP) to encrypt data communication; – upgrading Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access 2/3 (WPA2/WPA3) to enhance Wi-Fi security standards; and – disabling Server Message Block version 1 (SMBv1), as it has been superseded by more secured versions.	#	In situations where OT assets use weak protocols that cannot be replaced, the organisation shall implement compensating controls such as physical security (or isolation) or network segmentation.	#
A.6.4 (c)	Unused features, services, or applications shall be disabled or removed, e.g., disable file sharing services, File Transfer Protocol (FTP) service and restrict software macros.	#	#	#

A.6.4 (d)	The organisation shall ensure that third parties or contractors protect their own software, applications and environments used for service delivery to the organisation.	#	#	#
A.6.4 (e)	The organisation should review the cybersecurity posture of third parties or contractors, or perform audits on contractors, so as to adequately manage supply chain risk. NOTE – In Singapore, Cyber Essentials and Cyber Trust are certifications that help organisations to implement cybersecurity.	#	#	#
A.6.4 (f)	Automatic connection to open networks and auto-run features of non-essential programs (other than backup or virus and malware protection solutions) shall be disabled.	#	#	#
A.6.4 (g)	Logging shall be enabled for audit logs of events that can assist in detecting, understanding or recovering from an attack, e.g. user-level events such as user log-ins in file access.	The organisation shall enable audit logs of events for its cloud environment if such logging is supported.	OT system behaviour and traffic are typically more deterministic, repeatable, and predictable than IT systems. The organisation shall monitor the logs in the OT environment, as anomalies in a deterministic environment may indicate potential cybersecurity incidents, particularly in environments where potential vulnerabilities may not be mitigated in a timely manner through patching due to constraints such as the need to wait for maintenance schedules to perform	The organisation shall enable audit logs for its AI tools and services if such logging is supported.

<table>
<tr><td></td><td></td><td></td><td>patching, or legacy devices that cannot be patched.</td><td></td></tr>
<tr><td>A.6.4 (h)</td><td>The organisation should enable other system logs, application logs, security tool logs and outbound proxy logs.</td><td>#</td><td>#</td><td>#</td></tr>
<tr><td>A.6.4 (i)</td><td>As good practice, automatic lock/session log outs should be enabled after fifteen minutes of inactivity for the organisation’s assets. These include user sessions on laptops, servers, non-mobile devices, databases and administrator portals.</td><td>#</td><td>For OT assets where automatic lock/session log outs are not supported, the organisation may implement compensating controls such as physical access control.</td><td>#</td></tr>
<tr><td>A.6.4 (j)</td><td>If the scope of certification includes mobile devices and/or IoT devices:
<table><tr><td>Mobile devices – e.g., mobile phones, tablets</td><td>– Mobile devices should not be jail-broken or rooted.
– Mobile device passcodes should be enabled.
– Automatic mobile device locks should be activated after two minutes of inactivity.
– Mobile applications should only be downloaded from official or trusted sources, avoiding side-loaded applications.</td></tr><tr><td>IoT devices</td><td>– The network hosting IoT devices should be segregated from the network hosting the organisation’s assets and data.
– Security features should be enabled on IoT devices, e.g., disabling device auto-discovery and Universal Plug and Play (UPnP).</td></tr></table></td><td>#</td><td>The organisation should restrict or minimise the use of maintenance devices outside of the OT environment or connecting such devices to non-OT networks. These devices should be disconnected and any temporary connections should be removed after maintenance activities are completed.</td><td>#</td></tr>
</table>

		– When selecting IoT devices, the organisation should use devices that are labelled for cybersecurity where available. NOTE – In Singapore, the Cybersecurity Labelling Scheme provides a rating for the cybersecurity of IoT devices.			

A.7 Update: Software updates – Update software on devices and systems

A.7.1 Introduction

Software vendors regularly provide software updates that include new features and address newly discovered security vulnerabilities. Prompt installation of these software updates is crucial to prevent attackers from exploiting security vulnerabilities.

A.7.2 Applicability

Software within the scope of assessment and certification includes those installed in servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, IoT, storage solutions and virtualisation platforms.

A.7.3 Objective

To ensure the timely application of updates and patches to software and applications, thereby safeguarding devices and systems against security vulnerabilities.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.7.4 (a)	The organisation shall prioritise the implementation of critical or important updates for operating systems and applications (e.g., security patches), obtained from official or trusted sources (e.g., verified through hash or checksum), as soon as feasible.	The organisation shall refer to the cloud shared responsibility model with its CSP.	When prioritising the implementation of updates in the OT environment, the organisation shall assess:	#

		For SaaS, the organisation shall verify the CSP's responsibility for performing software updates and patch vulnerabilities within its software. For other cloud service models where the organisation is responsible, the organisation shall implement software updates and patch vulnerabilities on its cloud workloads.	– the applicability of, exposure to and severity of the vulnerabilities; – the potential impact on OT operation and safety; and – the availability of certified patches from vendors. The organisation shall develop a backup and rollback/restoration plan before performing patching or software upgrades to address potential update failures. Compensating controls should be implemented if patching is not feasible, e.g., patching disrupts or impacts operations significantly.	
A.7.4 (b)	The organisation should conduct compatibility tests on operating system and application updates before installation.	#	Such compatibility tests should be carried out, e.g., by the OT vendor, to assess the potential impact on OT operations or safety.	#
A.7.4 (c)	The organisation should consider enabling automatic updates for critical operating system and application patches where feasible so that they can receive the latest updates, and the deployment can be staggered into stages, starting with a subset of the organisation's assets.	#	For known, exploited vulnerabilities, the organisation should perform updates as soon as possible, factoring in when it is safe and appropriate to do so.	#

<table>
<tr><td></td><td></td><td></td><td>For less critical or urgent updates, the organisation may do so during scheduled maintenance windows or downtime, enabling automated or timely updates only when safe and appropriate.

Compensating controls should be implemented if patching is not feasible, e.g., patching disrupts or impacts operations significantly.</td><td></td></tr>
<tr><td>A.7.4 (d)</td><td>If the scope of certification includes mobile devices and/or IoT devices:

<table><tr><td>Mobile devices – e.g., mobile phones, tablets</td><td>– The organisation should ensure that updates and patches for mobile devices are only downloaded only from trusted sources (e.g., the official application store from the manufacturer).</td></tr><tr><td>IoT devices</td><td>– The organisation should remove or replace any IoT devices (e.g., CCTVs, printers) that are not receiving any software patches or updates.</td></tr></table></td><td>#</td><td>#</td><td>#</td></tr>
</table>

A.8 Backup: Back up essential data – Back up the organisation's essential data and store them separately and securely

A.8.1 Introduction

Data backups are critical for enabling quick recovery from cybersecurity incidents such as ransomware or malware, and physical disruptions such as system failures, theft, or natural disasters.

A.8.2 Applicability

Essential business information within the scope of assessment and certification refers to information necessary for restoring the organisation's services or operations.

A.8.3 Objective

To ensure the regular back up of all essential business information in a secure manner to enable the organisation to restore and recover business operations following cybersecurity incidents.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.8.4 (a)	The organisation shall identify and back up business-critical data and systems. This is guided by identifying the data and systems essential for business recovery in the event of a cybersecurity incident, as well as meeting contractual or regulatory requirements. Examples of business-critical systems include Customer relationship management (CRM) and enterprise resource planning (ERP). Examples of business-critical data include financial data, business transactions and source code.	The organisation shall perform backups of its business-critical data in the cloud, e.g., storing backups on hard disk drives, purchasing appropriate backup services, using multiple CSPs for backup.	For the OT environment, backup requirements are determined by identifying the information needed to support the recovery of OT operations. Examples include the state of key OT systems, data, configuration files, and programs at regular intervals to support recovery to a stable state.	#
A.8.4 (b)	For business-critical data and systems, backups shall be performed regularly, with the backup	#	The backup frequency shall commensurate with the rate	#

	frequency aligned to business requirements and the organisation's data loss tolerance.		of data change, e.g., sub-segments of the OT network with less dynamic data may not need such frequent backups.	
A.8.4 (c)	For non-business-critical systems or non-essential information, backups should still be performed albeit at a lower frequency or on a long-term basis.	#	#	#
A.8.4 (d)	The backup process should be automated where feasible.	#	In situations where automated backups are not appropriate or recommended, e.g., automated backups negatively impact OT operations or safety, the organisation may perform regular scheduled backups during scheduled maintenance windows or downtime.	#
A.8.4 (e)	If the scope of certification includes hardware assets such as mobile devices and/or IoT devices: Mobile devices – Essential business information stored on mobile phones, e.g., Short Message Service (SMS) conversations, important client contacts, should be automatically backed up and transferred to a secondary mobile phone or secondary storage.	#	#	#

	IoT devices – IoT devices containing essential business information, e.g., sensors in farms or healthcare, should be backed up manually where automatic backup is unavailable.			
A.8.4 (f)	All backups shall be protected from unauthorised access and restricted to authorised personnel only, e.g., password-protected storage media, tape storage at an alternative office location, encryption of backups. Backups should minimally be passphrase-protected.	#	#	#
A.8.4 (g)	Backups shall be stored separately and isolated from the operating-environment. Where feasible, backups should be stored offsite, e.g., password-protected USB flash drives, encrypted external hard disks, tape storage at an alternative office location.	The organisation's backup of its business-critical data in the cloud shall be stored separately, e.g., in on-premises storage or systems, utilising appropriate backup services, employing alternative CSPs.	#	#
A.8.4 (h)	Frequent backups, e.g., daily or weekly, should be stored online to facilitate quick recovery, e.g., cloud backup storage.	#	#	#
A.8.4 (i)	As good practice, backups should be tested at least bi-annually, or more frequently, to ensure effective restoration of business-critical data and systems.	#	For testing integrity of backups in situations where there redundant or spare OT equipment or systems are unavailable to support such testing, compensating controls such as hash or	#

			checksum validation should be implemented.	

A.9 Respond: Incident response – Be ready to detect, respond to and recover from cybersecurity and data breach incidents

A.9.1 Introduction

Cybersecurity incidents can significantly impact an organisation in terms of cost, productivity, and reputation. A robust cybersecurity incident response plan is essential for enabling the organisation to respond quickly and effectively by streamlining decision-making, outlining processes and defining appropriate use of available technologies during a cybersecurity incident.

A.9.2 Applicability

Cybersecurity incidents affecting the organisation's operating environment and assets, including employees and customers.

A.9.3 Objective

To ensure the organisation has an incident response plan that enables timely, professional, and appropriate detection, response, and recovery from cybersecurity incidents.

Clause	Classical Cybersecurity	Cloud Security	OT Security	AI Security
A.9.4 (a)	The organisation shall establish an up-to-date basic incident response plan to guide the organisation in responding to common cybersecurity and data incidents. Examples include ransomware, social engineering, data breach and distributed denial-of-service (DDoS) attacks. The plan shall contain details as follows:	The organisation shall include scenarios related to cloud-specific incidents in its incident response plan, e.g., accidental disclosure of data from the cloud. The organisation shall verify the obligations of its CSPs regarding cooperating in	The organisation shall include scenarios related to OT-specific incidents in its incident response plan, e.g.: – ransomware impacting OT environment; – supply chain risks arising from vendor access to the	The organisation shall include scenarios related to AI-specific incidents in its incident response plan, e.g., employees' disclosure of sensitive organisational information to external AI tools or services.

	– Clear roles and responsibilities for key personnel involved in the incident response plan process; – Procedures for detecting, responding to and recovering from common cybersecurity threat scenarios; and – A communication plan and timeline for escalating and reporting the incident to internal and external stakeholders (e.g., regulators, customers, senior management).	investigating and remediating incidents that have impacted or might impact the confidentiality, integrity, or availability of the organisation's data stored in the cloud, ensuring alignment with the organisation's requirements.	OT environment (on-site and remotely); – credential compromise, enabling compromised IT credentials to access the OT network; – breach of legacy unpatched OT devices; and – improper configuration of segmentation or firewalls. As part of incident response planning, the organisation shall obtain documentation of all error messages and error conditions from its OT vendors for inclusion in its incident response plan. This documentation shall be readily accessible in the event of an incident to enable the organisation to determine whether the incident is caused by an error condition or a cybersecurity incident. The organisation's incident response shall include recovery procedures to address: – partial recovery to a reduced/constrained operation to meet critical service objectives; and	

			– full recovery to the last operational state prior to the cybersecurity incident. The organisation's incident response plan shall be documented in paper form or on an offline system that cannot be compromised during a cyber incident.	
A.9.4 (b)	The incident response plan shall be communicated to all employees with access to the organisation's IT assets and/or environment.	#	This documentation shall include: – employees involved in operating, securing and maintaining the OT environment; – employees handling IT where IT and OT operations converge; and – vendors involved in securing and maintaining the OT environment.	#
A.9.4 (c)	The organisation should conduct post-incident reviews and incorporate learning points to strengthen and improve the incident response plan.	#	#	#
A.9.4 (d)	As good practice, the incident response plan should be reviewed at least annually.	#	#	#