CSA CYBERSECURITY CERTIFICATION

Cyber Trust mark

Date of Publication: 04-2025 (Second edition)

A publication by

CSA SINGAPORE

SG CYBER SAFE

CYBER TRUST

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

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 Trust 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" and "should"

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 Trust mark

4.1 Concepts and principles

The Cyber Trust mark standard is designed for larger or more digitally mature organisations that have progressed beyond basic cyber hygiene. These organisations may have higher risk levels and can invest in expertise and resources to manage and protect their IT infrastructure.

The primary objective of the Cyber Trust mark is to serve as a mark of distinction, recognising organisations that actively address cybersecurity risks and maintain an adequate level of cybersecurity within their environment. Beyond classical cybersecurity risks, the Cyber Trust mark also provides protection when organisations utilise digital technologies such as cloud, OT and AI.

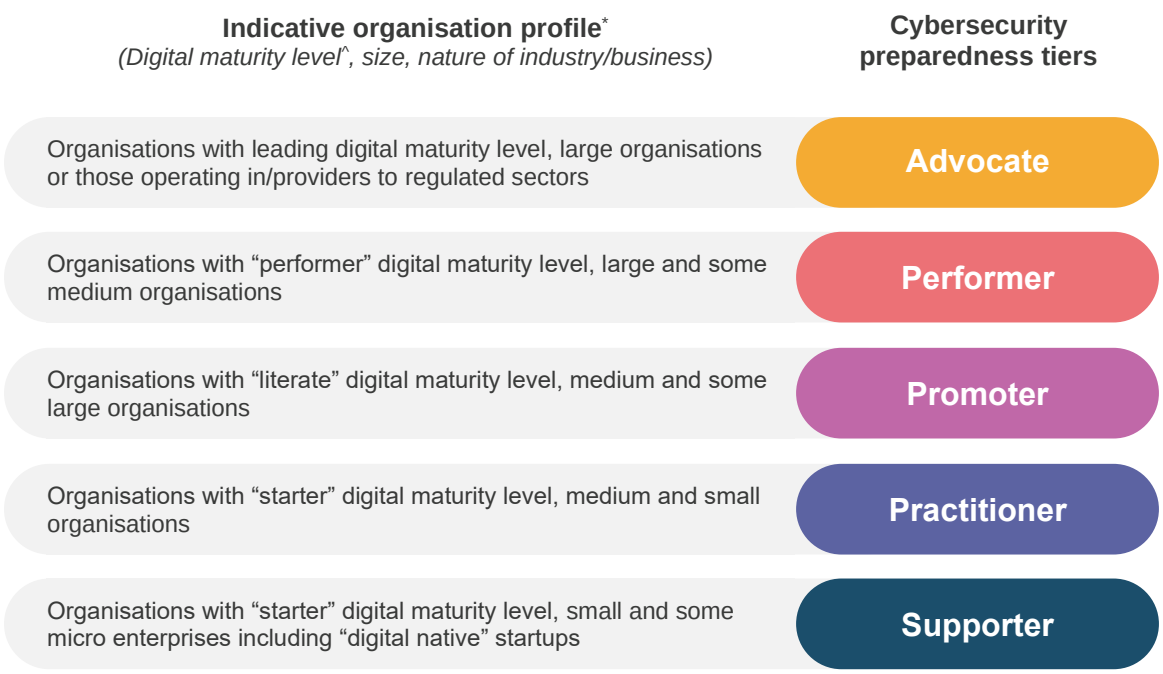
The Cyber Trust mark also serves as a pathway for organisations to adopt international standards (e.g., ISO/IEC 27001:2022 for information security management, ISO/IEC 27017:2015 for cloud security, IEC 62443 for industrial automation and control systems (IACS) security, or ISO/IEC 42001:2023 for AI management[5]).

Given the varying risk levels across organisations, the Cyber Trust mark adopts a risk-based approach rather than prescribing specific cybersecurity measures. This approach guides organisations in identifying gaps in their implementation of cybersecurity preparedness measures, ensuring their implementation aligns with their specific cybersecurity risk profiles.

The Cyber Trust mark certification comprises five cybersecurity preparedness tiers. Figure 1 shows the indicative target organisation profiles for each tier. Whilst indicative target organisation profiles for each tier are presented across dimensions such as digital maturity level, organisation size and nature of the industry/business, these are indicative and provide general guidance for organisations.

In reality, organisations of the same size may exhibit different risk profiles and, consequently, require different cybersecurity preparedness tiers due to variations in their sectors or the nature of data and/or cybersecurity breaches to which their operations are exposed to.

[5] The trust mark primarily focuses on the security of AI usage within organisations, which is part of a broader set of considerations for AI management.



* – *Organisations of the same size may have different risk profiles, and correspondingly, need to be at different cybersecurity preparedness tiers*
^ – *Description of digital maturity level aligns to terminology in IMDA Digital Acceleration Index (DAI)*

Figure 1 – Cyber Trust mark cybersecurity preparedness tiers and indicative organisation profiles

The Cyber Trust mark certification consists of twenty-two cybersecurity preparedness domains, each focusing on a specific cybersecurity theme. A series of cybersecurity preparedness statements are developed for each domain and organised across the five cybersecurity preparedness tiers. These statements articulate the cybersecurity measures that organisations should consider and implement, where relevant, to mitigate their inherent risks. Refer to Annex B for a complete list of cybersecurity preparedness domains and descriptions within the Cyber Trust mark.

Organisations at higher cybersecurity preparedness tiers shall meet a greater number of domains. This is illustrated in Figure 2.

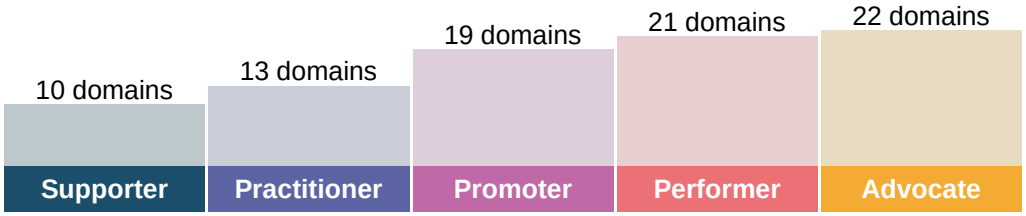


Figure 2 – Cyber Trust mark preparedness tiers and domains

Since different organisations have different business (and correspondingly, risk) profiles, the Cyber Trust mark certification provides a two-part assessment to guide organisations in the following:

a) Understanding their cybersecurity risk profiles, and

b) Identifying the relevant cybersecurity preparedness domains needed to mitigate these risks

4.2 Organisational profile

Organisations should assess whether their business needs align with the protection and/or recognition afforded by Cyber Trust mark certification.

The cybersecurity posture of an organisation is influenced by multiple factors and varies across organisations. The Cyber Trust mark does not mandate that organisations achieve a specific cybersecurity preparedness tier. Organisations should invest in relevant and appropriate cybersecurity measures that commensurate with their risk profiles.

4.3 Boundary of scope and statement of scope

4.3.1 Boundary of scope

Organisations shall establish the boundary of scope for certification and determine the assessable components of their environment for trust 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 the scope shall be clearly defined, including the following:

- Business services within scope;
- Business units involved;
- Network boundary;
- Devices and/or systems within scope;
- Software and/or services within scope; and
- Physical locations.

4.3.2 Statement of scope – Guiding principles

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:

- Organisation chart depicting the business units within scope;
- Context of the organisation's business;
- System and network diagram;
- Inventory listing of devices and/or systems;
- Inventory listing of software and/or services;
- Locations where the organisation operates or conducts services that are to be included within the scope of certification; and
- Cyber Trust mark self-assessment performed by the organisation.

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

[6] For organisations that implement BYOD, where employees use their personal mobile devices for company tasks to access the organisation's data or services, the scope of assessment and certification shall include such devices.
[7] For organisations that adopt cloud-based software, the scope of assessment and certification shall include such services.

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:

- 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;

- 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";

- Describe the location of operations of the organisation if it operates in multiple locations, e.g. "Management and operations supporting [key functions] in [location in a country, or the name of the country]"; and

- Describe a specific business function in the organisation, and gradually expanding the scope of certification over time.

4.3.3 Statement of scope – Cybersecurity pillar

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

- Classical cybersecurity;
- Cloud security;
- OT security; and/or
- 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"

4.4 How organisations can secure their usage of digital technologies

As end-user organisations embark on digitalisation, their attack surface expands. Organisations may begin by implementing cybersecurity measures within the Cyber Trust mark to protect themselves. Over time, the technology intensity 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, applicable to its IT systems, to also include OT security, for coverage of its OT systems.

Whilst the Cyber Trust mark is not intended for product certification, organisations that are providers of IT, cloud, OT or AI products and/or services may seek Cyber Trust mark certification. 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. For developers and/or providers of software products and/or solutions, they should consider an appropriate tier of certification that includes relevant domains for vulnerability assessment and secure software development life cycle (SDLC).

4.5 Pre-certification preparation by organisations

Before engaging a certification body, the organisation shall complete the guided self-assessment template required for Cyber Trust mark certification, as shown in Table 8.

This comprises a two-part assessment:

a) **Assessment of risk** – The organisation performs a risk assessment using the risk scenarios provided in the risk assessment template. These risk scenarios are derived from prominent/common cybersecurity incidents within organisations. Organisations assess their inherent risk, which represents the amount of risk faced by the organisation in the absence of any cybersecurity measures. This is achieved by evaluating the likelihood and impact of these scenarios occurring within their environment.

b) **Assessment of cybersecurity preparedness** – Concurrently with the assessment of the inherent risk of each risk scenario, the organisation reviews the corresponding cybersecurity preparedness domains mapped to the respective risk scenario. For each domain, the organisation shall identify the relevant or appropriate cybersecurity preparedness tier that reflects the practices implemented within the organisation.

By referencing the assessed cybersecurity preparedness tier for each domain, the organisation then evaluates its residual risk, which represents the risk faced by the organisation when mitigating cybersecurity measures are applied. The organisation shall also determine the risk treatment of the residual risks identified.

The outcome of the self-assessment provides the organisation with an estimated cybersecurity preparedness tier across the different domains, including a list of self-identified gaps against the applicable cybersecurity preparedness domain statements. The organisation should consider these gaps while assessing the residual risks for the various risk scenarios as part of the risk assessment. The organisation shall also develop appropriate risk treatment plans and remediation activities based on their risk profile.

Before engaging a certification body, the organisation may engage a consultant to conduct a pre-certification audit on the scope intended for certification.

Figure 3 illustrates the process flow for the organisation to complete the two-part self-assessment and undertake an optional pre-certification audit.

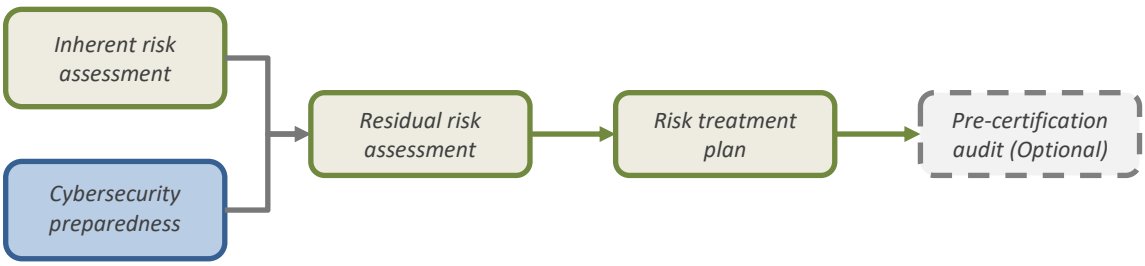


Figure 3 – Pre-certification preparation: Self-assessment and optional pre-certification audit

The Cyber Trust mark certification involves verification of implementation and effectiveness. Therefore, organisations applying for certification should ensure they have approximately three months of implementation data/logs in their systems by the time assessors conduct the verification of implementation and effectiveness.

4.6 Risk scenarios in assessment of risk

The risk assessment template is pre-populated with risk scenarios depicting prominent/common cybersecurity incidents within organisations. Organisations assess their inherent risk by evaluating the likelihood and impact of these scenarios occurring in their environments. The categories of risk scenarios include the following:

a) **Data breach**: Cybersecurity incidents where the organisation's information/data is stolen or accessed from a system without the organisation's knowledge or authorisation.

b) **Human factor**: Cybersecurity incidents resulting from human error, negligence or malicious insider activity.

c) **Infrastructure**: Cybersecurity incidents affecting the organisation's infrastructure, causing disruption to its operations.

d) **Physical security**: Cybersecurity incidents where weak physical security enables unauthorised access to the organisation's environment, systems and information by malicious individuals.

e) **Regulatory and compliance:** Non-compliance with regulatory standards applicable to the respective organisation.

f) **Supply chain**: Cybersecurity incidents where the organisation's third-party service providers are attacked as a means of targeting the organisation.

4.7 Assessment of inherent and residual risk

4.7.1 Mapping risk scenarios to cybersecurity preparedness domains

Table 1 provides a complete list of risk scenarios, including relevant information security properties, (e.g., confidentiality, integrity or availability) and applicable cybersecurity preparedness domains.

Organisations that have included cybersecurity, cloud security, OT security and AI security within their scope of certification shall minimally include the risks outlined in the respective sections of Table 1**.** Organisations may include additional risk scenarios as needed.

Table 1 – Mapping risk scenarios to cybersecurity preparedness domains

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
Cybersecurity risks				
1	Infrastructure	Attacker exploits an unpatched vulnerability in an obsolete operating system (OS) or a key application used by the organisation, and gains unauthorised access into a key corporate system to manipulate the system or application.	Confidentiality Integrity Availability	Domain: Risk management Domain: System security Domain: Vulnerability assessment
2	Infrastructure	Attacker floods the network with traffic and overwhelms its resources, resulting in the disruption or inaccessibility of critical services in the organisation.	Availability	Domain: Risk management Domain: System security Domain: Network security
3	Infrastructure	Attacker exploits a network or system with weak configuration (e.g., configuration left as default	Confidentiality Integrity Availability	Domain: Backups Domain: System security

[8] These refer to "confidentiality", "integrity" and "availability", commonly known as the "CIA triad". "Confidentiality" focuses on protecting information from unauthorised access. "Integrity" focuses on providing assurance that information is trustworthy, complete and accurate. "Availability" focuses on ensuring reliable access to information when this is needed.

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
		settings) and gains unauthorised access into the organisation's network or system.		Domain: Cyber threat management Domain: Network security
4	Infrastructure	Employees misconfigure a critical system in the organisation, resulting in an attacker exploiting this to cause disruption to key services or operations.	Availability	Domain: Audit Domain: Training and awareness Domain: Backups Domain: System security Domain: Business continuity /disaster recovery
5	Infrastructure	Attacker uses malware to attack the organisation's IT systems and penetrates its IT infrastructure, including servers and endpoints, and destroys sensitive and personal information.	Availability	Domain: Backups Domain: System security Domain: Virus and malware protection Domain: Cyber threat management Domain: Vulnerability assessment
6	Data breach	Attacker compromises an employee's credentials to gain access into the organisation's systems, performs lateral movement to systems storing critical or sensitive data to exfiltrate and encrypt the data, before issuing a ransom note to the organisation.	Confidentiality Integrity Availability	Domain: Access control Domain: Backups Domain: System security Domain: Network security Domain: Incident response
7	Data breach	Employee loses a corporate device or has it stolen, resulting in unauthorised users being able to access the organisation's confidential and/or sensitive data, leading to data leakage or disclosure of confidential and/or sensitive data.	Confidentiality	Domain: Risk management Domain: Training and awareness Domain: Asset management Domain: Data protection and privacy Domain: Access control Domain: Network security
8	Data breach	Attacker exploits a vulnerability in the organisation's application and gains access to extract confidential and/or sensitive data, including personal data.	Confidentiality	Domain: Risk management Domain: Data protection and privacy Domain: System security Domain: Secure SDLC Domain: Access control Domain: Vulnerability assessment Domain: Network security
9	Data breach	Attacker takes advantage of compromised or unauthorised devices to access the organisation's confidential and/or sensitive data, which leads to the leakage of confidential and/or sensitive data.	Confidentiality	Domain: Risk management Domain: Data protection and privacy Domain: Bring your own device (BYOD) Domain: System security Domain: Virus and malware protection Domain: Cyber threat management Domain: Network security

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
10	Data breach	Employee fails to properly manage or handle portable storage devices (e.g., Universal Serial Bus (USB) drives, external hard disks) to transfer confidential and/or sensitive data, resulting in unauthorised access to sensitive data.	Confidentiality	Domain: Training and awareness Domain: Asset management Domain: Data protection and privacy
11	Data breach	Unauthorised user is able to access data from IT assets that are not disposed of properly, resulting in disclosure of confidential and/or sensitive data.	Confidentiality	Domain: Audit Domain: Asset management Domain: Data protection and privacy
12	Human factor	Disgruntled employee performs unauthorised modification to sensitive information, resulting in disruption to business operations.	Integrity Availability	Domain: Risk management Domain: Training and awareness Domain: Access control
13	Human factor	Employee falls prey to phishing emails containing malicious payload (e.g., attachments, Uniform Resource Locator (URL)), resulting in either compromise of employees' credentials, or introduction of malware.	Confidentiality Integrity Availability	Domain: Risk management Domain: Training and awareness Domain: Access control Domain: Virus and malware protection Domain: Network security
14	Human factor	Employee with access to confidential and/or sensitive data inadvertently uploads the data to an external service (e.g., public data analytics service, generative AI service), leading to disclosure of such data.	Confidentiality	Domain: Training and awareness Domain: Data protection and privacy
15	Human factor	Employee involved in managing financial transactions is taken in by deepfake impersonation of senior management to execute high-value transactions, resulting in financial losses for the organisation.	Integrity	Domain: Governance Domain: Training and awareness Domain: Incident response
16	Human factor	High turnover rate of or inadequate cybersecurity staff, resulting in a lack of resources to manage cybersecurity.	Confidentiality Integrity Availability	Domain: Governance Domain: Cyber strategy
17	Physical security	Unauthorised user gains access to data processing/sensitive information storage facility due to inadequate physical access control, resulting in damage or destruction of critical systems and data.	Confidentiality Integrity Availability	Domain: Risk management Domain: Backups Domain: Physical/environmental security Domain: Network security
18	Physical security	Unauthorised user gains access to the organisation's system via an inadequately secured wireless network access point, resulting in extraction of personal and sensitive information.	Confidentiality	Domain: Risk management Domain: BYOD Domain: Access control Domain: Network security Domain: Physical/environmental security

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
19	Physical security	Unauthorised visitors are allowed physical entry into the organisation's restricted premises due to inadequate physical security, resulting in unauthorised access and operations disruption as systems are powered off maliciously or accidentally.	Confidentiality Integrity Availability	Domain: Training and awareness Domain: Physical/environmental security
20	Physical security	Physical environment of critical systems (e.g., temperature, moisture) is not adequately managed, resulting in disruption of operations.	Availability	Domain: Backups Domain: Physical/environmental security Domain: Business continuity /disaster recovery
21	Regulatory and compliance	Organisation fails to comply with personal data protection legal or regulatory requirements, resulting in financial penalties, leakage of personal data and reputational losses to the organisation.	Confidentiality	Domain: Risk management Domain: Compliance Domain: Audit Domain: Data protection and privacy
22	Regulatory and compliance	Organisation fails to comply with cybersecurity legal or regulatory requirements, resulting in financial penalties, operational disruption and reputational losses to the organisation.	Confidentiality Integrity Availability	Domain: Risk management Domain: Compliance Domain: Audit
23	Regulatory and compliance	Staff and vendors fail to comply with the organisation's security policies and processes, leading to non-compliance.	Confidentiality Integrity Availability	Domain: Policies and procedures Domain: Risk management Domain: Compliance Domain: Audit Domain: Training and awareness
24	Supply chain	Erroneous transactions, arising from the vendor's negligence, occur in the organisation's system, resulting in compromise of integrity of the transactions processed by the system and financial losses for the organisation.	Integrity	Domain: Risk management Domain: Third-party risk and oversight
25	Supply chain	IT vendor engaged by the organisation has not implemented good cybersecurity practices (e.g., improper handling of the organisation's sensitive data, vendor software contains unpatched vulnerabilities and/or uses open source software or libraries with malicious code), resulting in attackers gaining unauthorised access to the organisation's system and/or data.	Confidentiality Integrity Availability	Domain: Risk management Domain: Access control Domain: Cyber threat management Domain: Third-party risk and oversight Domain: System security Domain: Vulnerability assessment Domain: Network security
26	Supply chain	Attackers launch attacks on key third-party service providers used by the organisation, resulting in	Availability	Domain: Risk management Domain: Cyber strategy

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
		disruption to key services and operations.		Domain: Business continuity/disaster recovery
Cloud security risks				
1	Infrastructure	Attacker exploits an insecure interface or application programming interface API in the organisation's cloud service and gains unauthorised access to sensitive data or manipulates the organisation's cloud workloads.	Confidentiality Integrity Availability	Domain: Access control Domain: System security Domain: Secure SDLC Domain: Vulnerability assessment
2	Infrastructure	Organisation has not enabled adequate logging of cloud security events, which limits its ability to detect potentially malicious activities if attackers gain unauthorised access and attempt to disrupt the organisation's cloud workloads.	Availability	Domain: System security Domain: Cyber threat management
3	Infrastructure	Attacker exploits insecure configuration settings in the organisation's SaaS service and gains unauthorised access to manipulate the organisation's data or disrupt the delivery of the organisation’s cloud services.	Integrity Availability	Domain: Data protection and privacy Domain: System security
4	Data breach	Attacker exploits a database, cache or storage bucket that has weak configuration settings configured by developers in the organisation during the development stage that had not been tightened when the setup transitioned to the deployment stage, resulting in exposure of the entire database to data theft, destruction or tampering.	Confidentiality Integrity Availability	Domain: Audit Domain: Data protection and privacy Domain: System security Domain: Secure SDLC Domain: Access control
5	Human factor	Organisation has subscriptions with multiple cloud service models (e.g., a mix of SaaS, PaaS and IaaS) each managed by respective business units, with varying levels of employee awareness regarding their roles and responsibilities as cloud users versus those of their respective cloud services providers, resulting in insecure cloud practices among employees, such as expecting cloud service providers to be responsible for data backup.	Confidentiality Integrity Availability	Domain: Training and awareness Domain: Data protection and privacy Domain: System security
6	Human factor	Attacker compromises weak credentials used by an employee when accessing the organisation's cloud service (e.g., weak passphrases, compromised credentials that had been used for multiple accounts, or excessive	Confidentiality Integrity Availability	Domain: Training and awareness Domain: Data protection and privacy Domain: Access control

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
		access privileges granted to an employee) to gain unauthorised access to sensitive data that is stored in the organisation's cloud service.		
7	Supply chain	SaaS provider used by the organisation manages an insecure setup on the cloud (e.g., vendor software contains unpatched vulnerabilities and/or uses open source software or libraries with malicious code), resulting in attackers gaining unauthorised access to the organisation's data and cloud workloads through its provider.	Confidentiality Integrity Availability	Domain: Risk management Domain: Cyber threat management Domain: Third-party risk and oversight Domain: System security Domain: Vulnerability assessment Domain: Network security
8	Supply chain	Attackers launch attacks on a key cloud service provider used by the organisation, resulting in disruption to the organisation's services and operations as a large proportion of its cloud workload is with a specific cloud service provider.	Availability	Domain: Risk management Domain: Cyber strategy Domain: Business continuity/disaster recovery
OT security risks[9]				
1	Infrastructure	Attacker exploits a credential compromise in the organisation's IT network, which uses a centralised/shared credential management system across its OT and IT network, enabling the attacker to perform lateral movement to the OT network, resulting in disruption and/or manipulation of OT operations.	Safety Availability Integrity	Domain: Training and awareness Domain: System security Domain: Physical/environmental security Domain: Network security
2	Infrastructure	Attacker introduces malicious traffic into the OT environment through the IT network because of improper implementation or configuration of the network segmentation or firewall between the organisation's OT and IT network, resulting in disruption of OT operations.	Safety Availability	Domain: System security Domain: Virus and malware protection Domain: Physical/environmental security Domain: Network security
3	Infrastructure	Attacker bypasses the compensating control implemented to mitigate an unpatched vulnerability in a legacy OT device or system, and gains unauthorised access to the legacy OT environment, resulting in disruption and/or manipulation of OT operations.	Safety Availability Integrity	Domain: System security Domain: Physical/environmental security Domain: Vulnerability assessment Domain: Network security

[9] 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. Correspondingly, "safety" has been included under "information security properties".

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
4	Infrastructure	Attacker from a ransomware group exploits a vulnerability in the organisation's IT network. As the organisation's OT network relies on the IT system (e.g. for billing, tracking), when the IT system is impacted, the organisation's OT operations are disrupted and need to be shut down as well.	Safety Availability	Domain: System security Domain: Vulnerability assessment Domain: Network security Domain: Business continuity/disaster recovery
5	Infrastructure	Attacker exploits a vulnerability in a software or code library that has been implemented as a common software module in cross-sectoral OT deployments, resulting in large-scale cross-sectoral impact on OT operations, including disruption of the organisation's OT operations.	Safety Availability	Domain: System security Domain: Secure SDLC Domain: Physical/environmental security Domain: Vulnerability assessment Domain: Network security Domain: Business continuity/disaster recovery
6	Human factor	Employee overseeing OT operations connects a removable storage media with infected files to the organisation's OT network for routine on-site work without implementing any data sanitisation measures, resulting in virus/malware being introduced into the organisation's OT network and disruption of OT operations.	Safety Availability	Domain: Training and awareness Domain: Asset management Domain: BYOD Domain: System security Domain: Virus and malware protection Domain: Physical/environmental security Domain: Network security
7	Physical security	Attacker gains unauthorised access to the physical site hosting the OT environment as the organisation has not implemented adequate physical access control measures, resulting in disruption of its OT operations.	Safety Availability	Domain: Training and awareness Domain: Physical/environmental security
8	Supply chain	OT vendor engaged by the organisation connects the vendor maintenance laptop, which is infected by malware from other customer sites, to the organisation's OT network for routine on-site work without implementing any data sanitisation measures, resulting in infection of the organisation's OT network and disruption of OT operations.	Safety Availability Integrity Confidentiality	Domain: Asset management Domain: System security Domain: Virus and malware protection Domain: Third-party risk and oversight Domain: Physical/environmental security Domain: Network security
9	Supply chain	Remote access arrangement set up by the organisation for its OT vendor to provide remote maintenance and support is compromised due to a lack of Two-Factor Authentication (2FA), resulting in attacker gaining unauthorised entry to the organisation’s OT data and systems.	Safety Integrity Availability Confidentiality	Domain: System security Domain: Access control Domain: Third-party risk and oversight Domain: Network security

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
10	Supply chain	Attacker exploits a vulnerability in the cloud environment implemented by a third-party vendor engaged by the organisation to host and process its OT telemetry data in the cloud, resulting in the attacker gaining access to multiple OT sites that are cloud-managed.	Integrity Confidentiality	Domain: System security Domain: Virus and malware protection Domain: Third-party risk and oversight Domain: Vulnerability assessment Domain: Network security
AI security risks				
1	Infrastructure	Attacker launches a poisoning attack on the training data or run-time data that is input to the organisation's AI system or an AI service used by the organisation, resulting in manipulation of the output (e.g., recommendation, decision, prediction, content) from the AI system or service.	Integrity	Domain: Data protection and privacy Domain: System security Domain: Network security
2	Infrastructure	Attacker exploits a weakness in an insecure AI (e.g., Large Language Model (LLM)) plugin used by the organisation, resulting in injection of malicious content into the AI, or leakage of sensitive data such as credentials through the insecure plugin.	Confidentiality Integrity	Domain: Data protection and privacy Domain: System security Domain: Secure SDLC Domain: Network security
3	Infrastructure	Attacker provides high frequency, voluminous or malicious inputs to a LLM used by the organisation, resulting in a denial of service of the LLM.	Availability	Domain: Risk management Domain: System security Domain: Network security
4	Infrastructure	Attacker manipulates inputs into the organisation’s AI model such that the model misclassifies or misinterprets the inputs, changing its intended behaviour (i.e. model evasion), resulting in unintended outcomes.	Integrity	Domain: System security Domain: Secure SDLC Domain: Network security
5	Data breach	Attacker manipulates the behaviour of a LLM used by the organisation through direct or indirect prompts, resulting in unintended actions from the LLM such as the attacker gaining unauthorised privilege access to restricted parts of a system, altering system configuration or critical data records.	Integrity	Domain: System security Domain: Secure SDLC Domain: Network security
6	Data breach	Attacker queries the organisation's AI model extensively to monitor the input and output to understand its structure and decisions, before replicating it, resulting in model theft.	Confidentiality	Domain: System security Domain: Secure SDLC Domain: Network security

Risk ref	Risk type	Risk scenario	Information security properties[8]	Applicable cybersecurity preparedness domains
7	Human factor	Employee uses an authorised generative AI solution deployed in the organisation for generating summaries and insights, but has not verified the output generated before using this as top-line information, resulting in inaccurate information being communicated to internal (e.g., senior management) and external (e.g., customers) stakeholders.	Integrity	Domain: Training and awareness Domain: Data protection and privacy
8	Human factor	Employee submits proprietary information from its organisation (e.g. internal meeting minutes, source code) into an external generative AI tool or service that has not been authorized or approved by the organisation for productivity or optimisation, resulting in leakage of confidential or sensitive data.	Confidentiality	Domain: Training and awareness Domain: Data protection and privacy
9	Supply chain	Attacker exploits an AI model developed by the organisation's provider, or obtained from open source, that had been compromised with malicious code or contains a backdoor, resulting in unintended behaviour of the AI system, or the AI system posing a security risk to other systems, which can result in data leakage.	Confidentiality Integrity	Domain: Data protection and privacy Domain: System security Domain: Third-party risk and oversight Domain: Vulnerability assessment Domain: Network security
10	Supply chain	Attacker exploits a model that is not adequately secured, which has been developed by the organisation's provider, to launch an attack on the organisation, resulting in unintended behaviour of the AI system or data leakage.	Confidentiality Integrity	Domain: Data protection and privacy Domain: System security Domain: Third-party risk and oversight Domain: Vulnerability assessment Domain: Network security

4.7.2 Assessing inherent risk – Risk likelihood and impact

Organisations assess their inherent risk by evaluating the likelihood and impact of the risk scenario occurring within their environments. Each risk scenario shall have a value of likelihood and impact of risk assigned.

“Likelihood” refers to the probability of the risk scenario occurring. Organisations shall refer to Table 2 for guidance on assessing likelihood.

Table 2 – Assessment of the likelihood of risk scenario occurring

Likelihood	Likelihood score	Description	Indicative Probability (of occurrence in a year)
Highly likely	5	The event may occur in all circumstances	≥ 61 %
Likely	4	The event may occur in most circumstances	≥ 41 % – 60 %
Possible	3	The event should occur at some time	≥ 21 % – 40 %
Unlikely	2	The event may occur at some time	≥ 5 % – 20 %
Rare	1	The event may occur only in exceptional cases	< 5 %

"Impact" is assessed by the severity of harm to the organisation as a result of the risk scenario. Organisations shall refer to Table 3 for guidance on assessing impact.

Table 3 – Assessment of the impact of risk scenario occurring

Impact	Impact Score	Strategic	Financial	Operational	Regulatory Compliance (if applicable)	Brand value and Reputation
Major	5	Failure to meet key strategic objective; organisational viability threatened; major financial overrun.	Total financial failure, with inability to support organisation's operations.	Complete breakdown in service delivery with severe, prolonged impact on business operations affecting the whole organisation.	Large-scale action, material breach of legislation with very significant financial or reputational consequences.	Adverse publicity in local/ international media. Long-term reduction in public confidence.
Serious	4	Serious impact on strategy, major reputational sensitivity.	Disastrous impact on the financial exposure of the organisation, with long term damage incurred.	Significant impact on business operations and/or quality of service.	Regulatory breach with material consequences that cannot be readily rectified.	Adverse publicity in local/ international media. Short-term reduction in public confidence.
Significant	3	Significant impact on strategy, moderate reputational sensitivity.	Significant impact on financial exposure.	Large impact on customer experience and/or quality of service.	Regulatory breach with material consequences that cannot be readily rectified.	Criticism of an important process/service. Elements of public expectations not met.
Moderate	2	Moderate impact on strategy, minor reputational sensitivity.	Noticeable impact on financial exposure.	Moderate impact on business operations and/or quality of service.	Regulatory breach with minimal consequences that cannot be readily rectified.	Organisation's image tarnished with a specific group. Elements of public expectations not met.
Minor	1	Minor impact on strategy, minimal reputational sensitivity.	Negligible impact on financial exposure.	Negligible impact on business operations and/or quality of service.	Regulatory breach with minimal consequences and readily rectified.	Isolated case of damage to reputation. Potential for public concern/unlikely to warrant media converge.

4.7.3 Assessing inherent risk – Risk levels

The risk level for each risk scenario is determined by multiplying the risk likelihood score and the risk impact score. The description associated with each range of risk levels is outlined in Table 4.
.

Table 4 – Risk levels

Risk Measure	Risk Level	Risk Action	Description
17 – 25	Critical	Immediate action required to reduce the risk	Immediate risk treatment is required, and risk shall not be accepted. Risk treatment strategies shall be implemented immediately as the magnitude of impact can affect the survivability of the organisation or leave long-term damage to reputation and finances. The board and senior management shall be notified and updated frequently on the progress of the risk treatment.
13 – 16	High	Action required to reduce the risk	Immediate risk treatment is necessary, and risk shall not be accepted. Risk treatment strategies shall be implemented as the magnitude of the impact may immediately disrupt business operations or services provided to customers, leading to financial losses. The senior management shall be notified and updated frequently on the progress of the risk treatment.
10 – 12	Medium - High	Gradual action required to reduce the risk	Risk treatment is preferred, and risk should not be accepted. Risk treatment strategies should be implemented as the magnitude of impact can affect the organisation's long-term operations. The senior management shall be informed about the risk and updated periodically if the risk level increases.
5 – 9	Medium	Manage risk	Risk treatment is encouraged with the implementation of controls within the timeframe specified by the organisation. The organisation may want to monitor the risks regularly to detect any changes if any.
1 – 4	Low	Monitor/accept risk	The risk can be accepted as it falls within the organisation's risk appetite. Mitigating or compensating controls are already implemented to address the identified risk. Ongoing monitoring can be used to detect any changes in risk level.

4.7.4 Assessing residual risk

Organisations shall assess their residual risk after completing the assessment of their cybersecurity preparedness as specified in 0.

After completing this assessment, the organisation shall evaluate its residual risk, which represents the risk faced by the organisation when mitigating risk control measures are applied.

4.7.5 Risk heat map (for inherent and residual risk)

The resultant risk heat map that depicts the organisation's inherent risk is shown in Figure 4. A similar risk heat map is applicable for illustrating the organisation's residual risk.

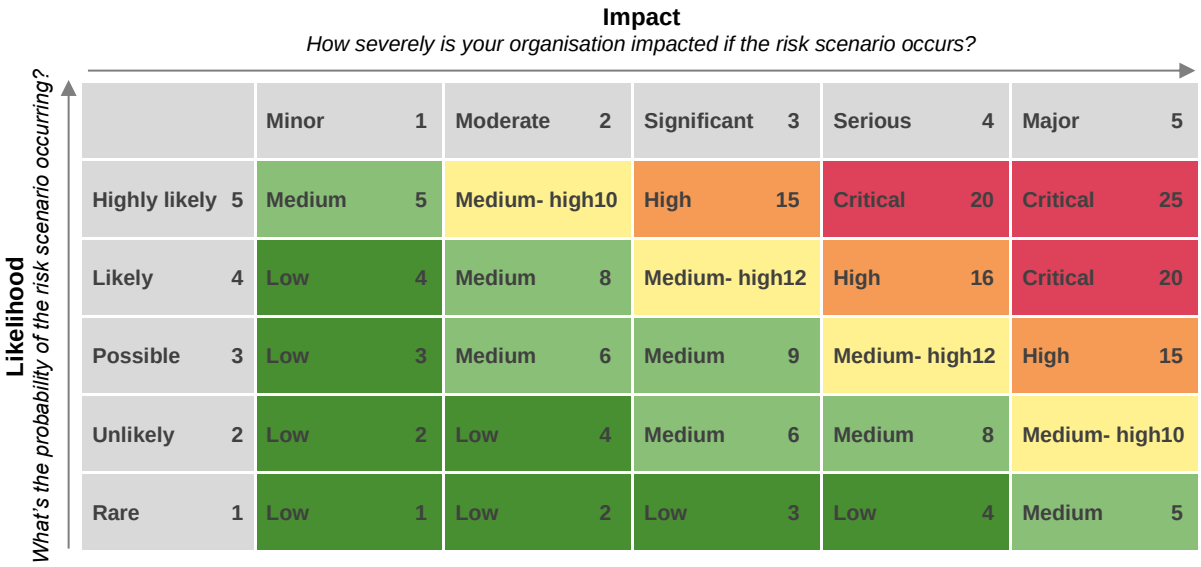


Figure 4 – Risk heat map

4.7.6 Treatment of residual risk

After the organisation has completed the assessment of its inherent risk (described in paragraphs 4.7.2 and 4.7.3) the assessment of the cybersecurity preparedness tier for each domain (described in paragraph 4.8), and the assessment of its residual risk (described in paragraph 4.7.4), the organisation shall derive the residual risk specific to each risk scenario.

Based on the residual risk level of each scenario, the organisation shall make a risk decision and propose the suggested treatment activity. The risk decisions are described in Table 5.

Table 5 – Risk decisions

Risk Option	Description
Accept	Knowingly and objectively accepting risks, provided they clearly satisfy the organisation's policy and the criteria for risk acceptance; and in view of the cost-effectiveness and business efficiency.
Mitigate	Applying appropriate controls to reduce the risk likelihood or impact, or both.
Avoid	Removing and eliminating the risk by removing the origin of the risk entirely. This treatment is not often applied unless terminating the activity which results in the risk arising does not materially affect the organisation.
Transfer	Implementing a strategy that transfers the risk to another party or parties, such as outsourcing the management of a service, developing contracts with service providers, or insuring against the risk. The third party accepting the risk shall be aware of and agree to accept this obligation, reducing the impact component of risk faced by the organisation.

4.7.7 Cyber Trust mark risk assessment template

The Cyber Trust mark risk assessment template is shown in Table 6.

Table 6 – Cyber Trust mark risk assessment template

Assessment of risk – Inherent risk						Assessment of cybersecurity preparedness		Assessment of risk – Treatment of residual risk									
			Inherent risk					Residual risk									
Risk ref.	Risk type	Risk scenario	Likelihood	Impact	Risk value and category	Applicable cybersecurity preparedness domains	Risk control measures set by the organisation	Likelihood	Impact	Risk value and category	Risk decision	Suggested treatment activity	Treatment owner	Target completion date	Current implementation status

4.8 Assessment of cybersecurity preparedness

4.8.1 Cybersecurity preparedness tiers

The assessment of an organisation's cybersecurity preparedness aims to document the cybersecurity measures that organisations should consider and implement, where relevant, to mitigate their risks.

Given the varying risk levels of organisations, the Cyber Trust mark adopts a risk-based approach instead of prescribing specific cybersecurity measures. This approach guides organisations in identifying gaps in their implementation of cybersecurity preparedness measures to ensure their implementation aligns with their cybersecurity risk profiles.

The Cyber Trust mark encompasses five cybersecurity preparedness tiers. Figure 1 shows the indicative target organisation profiles for each tier. The specific cybersecurity preparedness tier applicable to an organisation's profile is determined through a guided risk assessment process within the Cyber Trust mark certification.

The Cyber Trust mark certification comprises twenty-two cybersecurity preparedness domains. Each domain outlines a list of statements related to a specific cybersecurity theme that organisations should consider and implement, where relevant, to mitigate their inherent risks.

This means that there can be statements within a domain that may not be applicable to all organisations since their business needs and corresponding cybersecurity risk profiles can vary.

Figure 2 indicates that organisations at higher cybersecurity preparedness tiers shall meet a greater number of domains.

Table 7 illustrates the domains applicable for each cybersecurity preparedness tier.

Table 7 – Domains applicable for each cybersecurity preparedness tier

Tier	Supporter	Practitioner	Promoter	Performer	Advocate
Cyber governance and oversight					
1. Governance			●	●	●
2. Policies and procedure			●	●	●
3. Risk management	●	●	●	●	●
4. Cyber strategy					●
5. Compliance	●	●	●	●	●
6. Audit				●	●
Cyber education					
7. Training and awareness *	●	●	●	●	●
Information asset protection					
8. Asset management *	●	●	●	●	●
9. Data protection and privacy *	●	●	●	●	●
10. Backups *	●	●	●	●	●
11. Bring Your Own Device (BYOD)			●	●	●
12. System security *	●	●	●	●	●

Tier	Supporter	Practitioner	Promoter	Performer	Advocate
13. Anti-virus/anti-malware *	●	●	●	●	●
14. Secure Software Development Lifecycle (SDLC)			●	●	●
Secure access and environment					
15. Access control *	●	●	●	●	●
16. Cyber threat management				●	●
17. Third-party risk and oversight			●	●	●
18. Vulnerability assessment			●	●	●
19. Physical/environmental security		●	●	●	●
20. Network security		●	●	●	●
Cybersecurity resilience					
21. Incident response *	●	●	●	●	●
22. Business continuity/ disaster recovery		●	●	●	●
No of domains	10	13	19	21	22

* Measures in Cyber Essentials mark

The requirements and recommendations for the mark of cyber hygiene are mapped to the Supporter and Practitioner tiers respectively for Cyber Trust mark certification.

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

NOTE: Annex B contains the full list of cybersecurity preparedness domains and descriptions in the Cyber Trust mark.

4.8.2 Assessment of implementation of cybersecurity preparedness domains

As indicated in paragraph 4.7.1, the risk assessment template is pre-populated with risk scenarios depicting prominent/common cybersecurity incidents within organisations. The relevant cybersecurity preparedness domains applicable to each risk scenario are also listed to provide further guidance to organisations (See Table 1).

As the organisation completes the risk assessment for each risk scenario, it shall refer to the corresponding cybersecurity preparedness domains identified for that risk scenario to document the extent of implementation within the organisation.

The description of the statements in each cybersecurity preparedness domain is organised in escalating order – the statements begin with descriptions of more basic or rudimentary implementation and increase in the level of involvement or intensity.

For each domain, the organisation shall start with the statements in the lowest cybersecurity preparedness tier and indicate whether the cybersecurity measure indicated is implemented within its environment. If the organisation responds with “Yes”, the organisation shall progress to the next cybersecurity preparedness statement and/or tier. If the organisation responds with “No”, this indicates the organisation’s cybersecurity preparedness, and the organisation need not proceed to the next cybersecurity preparedness tier statement for that domain (see Table 8).

For statements that are not applicable to the organisation's environment (e.g., the cybersecurity measure is not needed as the process does not exist within the environment), the organisation may indicate these as "Not applicable". The organisation shall provide adequate justification as to why the risk and related statement are not applicable to its environment. This shall be validated subsequently by its appointed certification body.

If the organisation responds with "Not applicable" and provides adequate justification, it shall proceed to the next cybersecurity preparedness statement and/or tier for that domain.

As the key principles of cybersecurity are generally applicable across digital technologies like cloud, OT[10] and AI, the cybersecurity preparedness statements articulated under classical cybersecurity similarly apply to cloud, OT and AI security. If these are included in the scope of certification, the cloud-, OT- or AI-specific statements that contextualise the classical cybersecurity statements within that digital technology environment are indicated explicitly. 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.

Table 8 - Example of organisation progressively filling in a cybersecurity preparedness tier template

Preparedness tier	**Description**				**Organisation response** *(Yes, No, Not applicable)*	**Justification** *(if "Not applicable")*
	Classical Cyber-security	**Cloud security**	**OT security**	**AI security**		
Supporter	*Description*	*Cloud-specific description*	*OT-specific description*	*AI-specific description*		
Practitioner	*Description*	*Cloud-specific description*	#	#		
Promoter	*Description*	*Cloud-specific description*	*OT-specific description*	#		
Performer	*Description*	#	#	*AI-specific description*		
Advocate	*Description*	#	*OT-specific description*			

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.

4.8.3 Assessment of an organisation cybersecurity's preparedness tier

Upon completion of the risk assessment process, the organisation shall also have correspondingly completed its documentation of the cybersecurity measures implemented in the cybersecurity preparedness tier template.

As indicated in paragraph 4.7.6, after the organisation has completed the assessment of its inherent risk (described in paragraphs 4.7.2 and 4.7.3) the assessment of the cybersecurity preparedness tier for each domain (described in paragraph 4.8), and the assessment of its residual risk (described in paragraph 4.7.4), the organisation shall derive the residual risk specific to each risk scenario.

Based on the residual risk level of each scenario, the organisation shall make a risk decision and propose the suggested treatment activity.

[10] 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.

4.9 Independent assessment by a certification body

4.9.1 Approach and methodology for assessment

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

When assessors from the organisation's selected certification body evaluate the organisation's application for certification, the assessors shall apply professional judgement based on the organisation's business context, critical services provided, and information assets it holds to identify significant risk scenarios that the assessor should focus on during the assessment.

Assessors shall employ a combination of assessment techniques, including review and inspection of documents and other artefacts, conducting interviews, and on-site verification of implementation to assess the test of design, implementation and effectiveness of the organisation's cybersecurity security measures against the Cyber Trust mark cybersecurity preparedness statements.

4.9.2 Staged assessment approach

Assessors shall implement a two-stage approach for performing the assessment as follows:

a) **Verification of documentation (stage 1)** – An initial assessment to evaluate the relevant documentation and design of the cybersecurity measures implemented by the organisation. This stage typically involves reviewing the documentation prepared by the organisation to articulate its design considerations, policies, practices and/or implementation approach.

b) **Verification of implementation and effectiveness (stage 2)** – A more detailed assessment to evaluate the implementation and effectiveness of the cybersecurity measures implemented. This stage typically involves on-site inspection to verify the implementation and effectiveness of the organisation's cybersecurity measures indicated in its documentation.

For organisations whose scope of certification is multi-site, i.e., the organisation carries out its critical services and operations across more than one location, the assessment shall correspondingly involve multiple sites as defined in the scope of certification.

In stage 1 of the assessment, assessors may potentially identify gaps (e.g., major non-conformity) that require the organisation to take corrective actions prior to proceeding to stage 2.

Between stage 1 and stage 2, assessors typically allow time (e.g., six months) for organisations to take the necessary corrective actions to address the gaps identified. If this period is exceeded, the findings from the stage 1 assessment shall be deemed invalid, and the stage 1 assessment shall be conducted again.

In stage 2 of the assessment, organisations shall ensure that they have approximately three months of implementation data/logs in their systems so that assessors can perform verification of implementation and effectiveness.

4.9.3 Guiding principles for issuance of Cyber Trust mark certification tiers

The cybersecurity preparedness tier for each domain is determined by identifying the tier where the organisation has implemented the relevant cybersecurity measures to address the majority of the cybersecurity preparedness statements.

For the organisation to achieve a cyber preparedness tier *n*, the organisation shall achieve the following:

a) For the "Supporter" tier (i.e., $n = 1$): The organisation shall meet all the cybersecurity preparedness statements indicated, i.e., 100 % "Yes" responses.

b) From tier 1 to tier *n*: There shall not be any cybersecurity preparedness statements not met by the organisation, i.e., 0 % “No” responses, which means 100 % of the responses are either “Yes” or “Not applicable”.

c) From tier 1 to tier *n*: The total number of “Not applicable” responses to the cybersecurity preparedness statements shall be < 20 %.

d) From tier 1 to tier *n*: The total number of “Yes” responses to the cybersecurity preparedness statements shall be ≥ 80 %.

When the organisation’s selected certification body evaluates its application for certification, the assessors from the certification body shall assess the organisation for this tier in the two stages of assessment.

4.9.4 Certification life cycle

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

The organisation shall undergo surveillance audit assessments against its Cyber Trust mark certification tier annually. This ensures the organisation’s practices consistently meet the applicable Cyber Trust mark cybersecurity preparedness statements for the applicable tier. Upon expiration of the three-year Cyber Trust mark certification validity period, the organisation may choose to renew its Cyber Trust mark certification.

5 References

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

1. IEC 62443 series on security of industrial automation and control systems
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements
3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
4. ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
5. ISO/IEC 42001:2023 Information technology – Artificial intelligence – Management system
6. Baseline cyber security controls for small and medium organisations V1.2 by Canadian Centre for Cyber Security
7. CIS controls v8 by Centre for Internet Security (CIS)
8. CIS controls v8 cloud companion guide by CIS
9. CIS password policy guide by CIS
10. CISA cyber resilience review (CRR) by Cybersecurity & Infrastructure Security Agency and Carnegie Mellon University’s Software Engineering Institute, CERT Division
11. Cyber Essentials and Cyber Trust mark (2022) by Cyber Security Agency of Singapore
12. Cyber Essentials by UK National Cyber Security Centre
13. Cyber risks associated with generative artificial intelligence by Monetary Authority of Singapore (MAS)
14. Cybersecurity maturity model certification by U.S. Department of Defence
15. Cybersecurity playbook for large language model (LLM) applications by Government Technology Agency
16. Essential Eight by Australian Cyber Security Centre
17. Cybersecurity assessment tool by Federal Financial Institutions Examination Council
18. Federal Risk and Authorization Management Program (FedRAMP) by U.S. General Services Administration
19. HITRUST by Health Information Trust Alliance

20. NIST SP 800-82r3 Guide to operational technology (OT) security by National Institute of Standards and Technology (NIST)
21. Payment card industry data security standard (PCI DSS) by Visa, MasterCard, Discover Financial Services, JCB International and American Express
22. System and Organization Controls (SOC) for service organisations by American Institute of Certified Public Accountants
23. Technology risk management guidelines by MAS
24. The five ICS cybersecurity critical controls by SANS Institute
25. The NIST cybersecurity framework (CSF) 2.0 by NIST

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

Annex A
(normative)

Cyber Essentials mark — Requirements and recommendations

For information on Cyber Essentials mark, please visit go.gov.sg/cyber-essentials-certification.

Annex B
(normative)

Cyber Trust mark — Cybersecurity preparedness domains and descriptions

The following tables outline the cybersecurity preparedness domains and corresponding descriptions.

NOTE – For organisations in Singapore, clauses in the tables are cross-referenced to the CSA Cyber Trust mark certification document at https://www.csa.gov.sg/cyber-trust.

The key principles of cybersecurity apply broadly to 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 those environments are indicated explicitly. Where there is no digital technology-specific clause indicated, and a "#" symbol is used, the relevant classical cybersecurity statement also applies in that context.

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.

B.1 Domain: Governance

This domain ensures senior management is involved in the organisation's cybersecurity governance. This includes overseeing the development and implementation of a cybersecurity strategy and roadmap to define and track goals/objectives.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.1.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel includes content on cultivating	#	#	#

		cybersecurity leadership and setting cybersecurity direction for the organisation.			
B.1.2	**Practitioner**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership and setting cybersecurity direction for the organisation.	#	#	#
B.1.3	**Promoter**	The organisation has established and implemented practices to develop the importance of cybersecurity[11] within its business context and communicate this to all relevant stakeholders, such as employees, customers and partners.	As part of these practices, the organisation has established and implemented the cloud shared responsibility model with the CSP, e.g., through its commercial agreement with the CSP to establish clear roles and responsibilities between the organisation and the CSP.	#	Such practices include establishing mechanisms for: – The organisation to provide necessary security information about its AI systems to users and other relevant stakeholders, e.g. acceptable use policy of the AI systems in the organisation; and

[11] Cybersecurity includes cloud security, OT security and AI security if the organisation has included these areas in the scope of certification.

					– Employees and external parties to report AI security concerns of the AI systems in the organisation.
B.1.4	**Performer**	The organisation has defined and allocated the roles and responsibilities to ensure that it is clear who is responsible (e.g. Chief Information Security Officer (CISO)) to oversee the cybersecurity program implementation and manage cybersecurity risks within the organisation.	#	To ensure OT security has the attention of senior leadership, the organisation has identified member(s) of senior management to oversee and be overall responsible for both IT and OT security.	The organisation has defined and allocated roles and responsibilities for AI security due to the multidisciplinary nature of AI, which can cut across various organisational functions, e.g. functions overseeing ethics, legal matters, and risk areas.
B.1.5		The Board and/or senior management have sufficient expertise in cybersecurity and are involved in approving and overseeing the implementation of cybersecurity strategy, policies and procedures, and risk management actions.	The Board and/or senior management should have sufficient expertise in cloud security to make appropriate business decisions that take into consideration the implications associated with the specific risks of cloud computing, e.g., cloud concentration risk.	The Board and/or senior management should have sufficient expertise in OT security to make appropriate business decisions that take into consideration the implications associated with the specific risks associated with OT, e.g., continued deployment of legacy OT systems that may not adequately support cybersecurity.	The Board and/or senior management should have sufficient expertise in AI security to make appropriate business decisions that take into consideration the implications associated with the specific risks of AI, e.g., over-reliance on AI.
B.1.6		The organisation has established cybersecurity goals/objectives that are reviewed and approved by the Board and/or senior	#	#	This includes identifying and documenting the objectives to guide the secure use of AI system(s) and ensuring

		management at least annually and implemented through policies and procedures.			these system(s) are used according to the intended purposes.
B.1.7	**Advocate**	The Board and/or senior management has established a dedicated cybersecurity committee/forum to discuss on cybersecurity initiatives and activities regularly, oversee and monitor cybersecurity risks to ensure compliance with organisational cybersecurity policies, procedures and regulatory requirements.	The cybersecurity committee/forum has implemented measures to stay updated on cloud security practices, e.g., participating in cloud special interest groups.	The cybersecurity committee/forum has implemented measures to stay updated on OT security practices, e.g., participating in OT special interest groups.	The cybersecurity committee/forum has implemented measures to stay updated on fast-evolving AI security practices and governance landscapes, e.g., participating in AI special interest groups.
B.1.8		The organisation has established and implemented practices to ensure the Board and/or senior management are regularly updated on cybersecurity matters and key topics and decisions with regard to implementation of programmes and initiatives based on the organisation's cybersecurity risks are discussed and made promptly.	#	#	#

B.2 Domain: Policies and procedures

This domain ensures that cybersecurity policies and standards are established, implemented and communicated effectively. This provides employees with clear guidance on secure practices to protect the organisation's environment. Formalised policies and procedures also enable continuous review and update, monitoring for non-compliance and management involvement, to address the evolving cyber threat landscape.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.2.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership in the organisation, educating employees on cybersecurity, protecting its information assets, securing its access and environment, and ensuring that its business is cyber resilient.	#	#	#
B.2.2	**Practitioner**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel	#	#	#

		include content on cultivating cybersecurity leadership in the organisation, educating employees on cybersecurity, protecting its information assets, securing its access and environment, and ensuring that its business is cyber resilient.			
B.2.3	**Promoter**	The organisation has implemented practices to regularly communicate and update its employees on the cybersecurity processes, industry best practices and standards adopted to manage cybersecurity risks and measures to be taken to protect its information assets.	#	The organisation has implemented cross-functional or cross-team communications in areas where OT and IT security operations converge, to bridge the gaps, as OT and IT teams in the organisation may be distinct and operate independently.	The organisation has implemented cross-functional or cross-team communications in areas where AI security intersects with other functional areas in the organisation, due to the multidisciplinary nature of AI.
B.2.4	**Performer**	The organisation has established and implemented policies and procedures that incorporate the relevant requirements, guidance and directions to manage cybersecurity risk and protect information assets in its environment to ensure that employees have clear direction and guidance.	#	The organisation has established and implemented policies and procedures for the secure use of its OT environment and integrated these policies and procedures with its IT policies and procedures, whilst taking into consideration the differences between the OT and IT environment.	The organisation has established and implemented policies and procedures for the secure use of its AI system(s) in the organisation and integrated these policies and procedures with other organisational policies and procedures, e.g., enterprise and/or cybersecurity risk management.
B.2.5		The cybersecurity policies and procedures are approved and formalised by the Board and/or	#	#	#

		senior management to ensure top-down support.			
B.2.6		The cybersecurity policies and procedures are published, communicated and made accessible for employees to ensure that the employees have clear direction and guidance to perform their work securely.	#	#	#
B.2.7	**Advocate**	The organisation performs regular review and reporting on the effectiveness and deviations of its cybersecurity policies and procedures to the Board and/or senior management at least annually to ensure that they are kept informed.	#	#	#
B.2.8		The organisation has established and implemented the necessary measures to ensure compliance with its cybersecurity policies and procedures.	#	#	This includes policies and processes to ensure the secure use of AI system(s) and in accordance to organisational policies, including defining and documenting the processes for the secure use of AI system(s).
B.2.9		The organisation has established and implemented the necessary measures to track and monitor non-	#	#	#

		compliance with policies, processes and procedures, and to address associated cybersecurity risks.			

B.3 Domain: Risk management

This domain ensures the organisation has established risk management practices to identify, assess, mitigate, monitor and report cybersecurity risks.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.3.1	**Supporter**	The organisation has identified the cybersecurity risks in the environment, including risks on-premises, and where applicable, remote risks, to ensure that all the identified cybersecurity risks can be addressed.	The organisation has included cloud-specific risks, including: – how storing data in the cloud (which may span multiple jurisdictions) can impact data sovereignty and privacy requirements on the organisation; and – supply chain risks, as cloud services are often built on a series of CSPs.	The organisation has included OT-specific risks, including sector-specific risks based on incidents that have impacted its industry.	The organisation has included AI-specific risks, including: – risk of data leakage arising from both malicious attacks and unintended data disclosure by employees; and – risk of compromise to the integrity of data and/or the AI model, resulting in unintended output from its AI system(s) and has included mechanisms to provide adequate human oversight over the organisation's AI system(s).

B.3.2		The organisation performs steps to analyse and prioritise the critical cybersecurity risks in its business environment to ensure that the more critical cybersecurity risks are addressed first.	#	In an OT environment, such critical cybersecurity risks can include impact on human safety and potential physical impact on OT system(s). The organisation has put the priority on safety, systems reliability and physical assets.	#
B.3.3	**Practitioner**	The organisation has established and implemented a risk treatment plan with the guidelines and/or requirements to accept, remediate or mitigate the identified cybersecurity risks to ensure that cybersecurity risks are treated.	#	#	#
B.3.4		The organisation performs regular cybersecurity risk identification at least on an annual basis or whenever there are changes to the environment and tracks them to maintain a record of the cybersecurity risks in the environment.	#	#	#
B.3.5	**Promoter**	The organisation has defined and applied a cybersecurity risk assessment process to identify risk, assess the dependencies and evaluate the current measures in place to ensure that the organisation is	#	#	The organisation's cybersecurity risk assessment for its AI systems has factored in and documented the resources utilised, e.g.: – data assets;

		clear on how to assess the cybersecurity risks.			– software assets; – systems and computing resources; and – employee use of AI to fully understand the risks and impact.
B.3.6		The organisation has established, implemented and maintained a cybersecurity risk register containing the risks identified with their priority, the treatment plan, timeline, the employee(s) assigned the task of tracking and monitoring.	The organisation may use a standard risk register to track cloud services and deployments.	The risk register shall capture OT security risks that may not be mitigated due to the nature of the OT environment, e.g., insecure and/or outdated protocols, systems that are no longer supported, delays in updates due to maintenance schedules.	#
B.3.7	**Performer**	The organisation has established and implemented risk management policies and procedures with the requirements, guidelines and detailed steps to identify, analyse, evaluate, monitor and treat cybersecurity risks.	#	#	#
B.3.8		The organisation has defined and allocated roles and responsibilities for conducting and overseeing cybersecurity risk assessment to ensure that employees are clear on the tasks assigned to them.	#	#	#
B.3.9		The organisation has established the cybersecurity	Where there are major or significant cloud security	Where there are major or significant OT security risks	Where there are major or significant AI security risks

		risk appetite and cybersecurity risk tolerance statement approved by the Board and/or senior management to ensure that there is organisational consensus on the type and acceptable level of cybersecurity risk.	risks that may not be mitigated, e.g., cloud concentration risks, the trade-offs and appropriate cyber resilience measures shall be reported to and approved by the Board and/or senior management.	that may not be mitigated, e.g., continued deployment of legacy OT systems that may not adequately support cybersecurity, the trade-offs and appropriate use of compensation controls shall be reported and approved by the Board and/or senior management.	that may not be mitigated, e.g., AI concentration risks, AI over-reliance, the trade-offs and appropriate mitigation measures shall be reported to and approved by the Board and/or senior management.
B.3.10	**Advocate**	The organisation has established and implemented a cybersecurity risk management framework that is integrated as part of the organisation's overall risk management to ensure alignment with business goals.	#	#	#
B.3.11		The organisation has established and implemented policy and process to report identified cybersecurity risks to the Board and/or senior management at least on a monthly basis to ensure that they are kept informed.	#	#	#
B.3.12		The organisation has established and implemented policy and process to review deviations to ensure that the residual cybersecurity risk stays within its cybersecurity risk appetite and risk tolerance level.	#	#	For the organisation implementing AI systems, its policies and processes to review deviations have included ways to monitor for data and model drift that may impact the ability of the model to meet

					intended outcomes, resulting in changes in AI risk exposure.

B.4 Domain: Cyber strategy

This domain ensures the organisation has established a cybersecurity strategy, supported by a detailed roadmap and workplan, to achieve planned targets and objectives within a specified timeframe and maintain organisation-wide cyber resilience.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.4.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership and setting cybersecurity direction for the organisation.	#	#	#
B.4.2	**Practitioner**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally.	#	#	#

		NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership and setting cybersecurity direction for the organisation.			
B.4.3	**Promoter**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership and setting cybersecurity direction for the organisation.	#	#	#
B.4.4	**Performer**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for	#	#	#

		organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership and setting cybersecurity direction for the organisation.			
B.4.5	**Advocate**	The organisation has established a cybersecurity strategy to achieve cyber resiliency and protect the organisation against cybersecurity threats in terms of people, process and technology. The cybersecurity strategy has been translated into a roadmap to achieve planned targets over a time period.	The cybersecurity strategy has included: – business continuity and cyber resilience strategies which are developed based on the cloud service model(s) between the organisation and its CSPs; and – infrastructure design and decisions.	The cybersecurity strategy and roadmap has taken into account: – cybersecurity goals for its OT systems, such as focusing on safety, reliability and the physical systems and processes; – the long lifecycle of OT assets; and – the organisation's operational model for OT, e.g., insource, outsource, and/or use of managed security services.	The cybersecurity strategy and roadmap has identified and documented the organisation's objectives to guide the secure use of its AI system(s).
B.4.6		The organisation has established and implemented a cybersecurity workplan based on its cybersecurity strategy and roadmap, incorporating the necessary actions, timelines and allocated resources to achieve the planned targets.	#	#	#
B.4.7		The organisation has allocated sufficient budget and funds to achieve the planned	#	#	#

		cybersecurity targets. The budgets and funds are monitored by the Board/senior management and revised on a regular basis based on updates received.			
B.4.8		The organisation has tracked and evaluated its progress on cybersecurity strategy, the roadmap and workplans regularly at least on an annual basis with its Board/senior management to ensure that they are updated on the progress and status.	#	#	#
B.4.9		The organisation has reviewed and updated its cybersecurity strategy, roadmap and workplan at least annually to ensure alignment with business goals and objectives and to factor in the evolving cyber threat landscape.	The organisation has also factored in the cloud threat landscape, where adversaries are targeting cloud services as more organisations implement cloud-based solutions.	The organisation has also factored in the OT threat landscape, which is seeing increased adversarial interest in OT.	The organisation has also factored in the AI threat landscape, as organisations increasingly adopt AI.

B.5 Domain: Compliance

This domain ensures the organisation is aware of applicable laws, regulations and guidelines related to cybersecurity, so that compliance can be achieved. A compliance policy with active identification of non-compliance allows the organisation to manage the associated risks.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security

B.5.1	**Supporter**	The organisation has identified the cybersecurity-related laws, regulations and/or guidelines (e.g., sector-specific) applicable in its area of business in order to comply with them.	In identifying the relevant laws, regulations and/or guidelines, the organisation has considered how its cloud deployment, including the storage of data in the cloud, may span different legal and regulatory jurisdictions, and these may have their respective data privacy frameworks, or sector-specific frameworks, e.g., healthcare, financial sector.	In identifying the relevant laws, regulations and/or guidelines, the organisation has also considered the applicable safety laws, regulations and/or guidelines.	In identifying the relevant laws, regulations and/or guidelines, the organisation has factored in the emerging landscape of AI regulations in the countries it operates in.
B.5.2	**Practitioner**	The organisation has established and implemented measures to ensure compliance with the applicable cybersecurity-related laws, regulations and/or guidelines, e.g., sector-specific.	#	#	#
B.5.3	**Promoter**	The organisation has communicated cybersecurity-related laws, regulations and/or guidelines, (e.g., sector-specific) to employees to ensure that they are aware of them when performing their tasks.	#	#	#
B.5.4		The organisation has defined and applied a process to ensure that they stay compliant and up to date with the latest cybersecurity-related laws, regulations and/or guidelines	#	#	#

		(e.g., sector-specific) applicable to the organisation.			
B.5.5	**Performer**	The organisation has established and implemented policy and procedures with the necessary measures, requirements and steps to address cybersecurity-related laws, regulations and/or guidelines, (e.g., sector-specific).	#	#	#
B.5.6		The organisation has defined and allocated roles and responsibilities to address the requirements in cybersecurity-related laws, regulatory compliance and/or guidelines (e.g., sector-specific) in the organisation to ensure that employees are clear of their tasks for compliance.	#	#	#
B.5.7	**Advocate**	The organisation has established and implemented a policy and process to ensure that the organisation's processes and systems comply with applicable cybersecurity-related laws, regulatory compliance and/or guidelines (e.g., sector-specific) and to identify any non-compliance.	#	#	#
B.5.8		The organisation has established and implemented	#	#	#

		the policy and procedure to take action against non-compliance with cybersecurity-related laws, regulations and/or guidelines (e.g., sector-specific) to ensure that the organisation is able to stay compliant.			
B.5.9		Cybersecurity-related laws, regulatory compliance and/or guidelines (e.g., sector-specific) and non-compliance are reported to the Board and/or senior management on a timely basis to ensure that they are kept informed of the associated risks and potential areas of non-compliance.	#	#	#

B.6 Domain: Audit

This domain ensures the organisation has established an audit program to assess the effectiveness of policies, processes, procedures and controls against cybersecurity risks.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.6.1	**Supporter**	Domain is not assessable for this tier.	#	#	#
B.6.2	**Practitioner**	Domain is not assessable for this tier.	#	#	#

B.6.3	**Promoter**	Domain is not assessable for this tier.	#	#	#
B.6.4	**Performer**	The organisation has established, implemented and maintained a cybersecurity audit plan, including at a minimum, the objective, scope, roles and responsibilities, guidelines, and frequency for auditing to assess the effectiveness of the organisation's policies, processes, procedures and controls against cybersecurity risks.	#	#	#
B.6.5		The organisation has established an internal audit function and/or team to assess the policies, processes, procedures and controls against cybersecurity risks.	#	#	#
B.6.6		The organisation has established and implemented policies, processes, procedures and controls to mitigate and address the audit findings based on priority and timelines to ensure that the audit findings are remediated promptly.	#	The organisation has established and implemented appropriate compensating controls to mitigate and address the audit findings that arise as a result of limitations in the OT environment, which prevent it from implementing adequate cybersecurity, e.g., constraints in using encryption due to potential time-sensitivity challenges, constraints in updating software to patch	#

				vulnerabilities promptly due to potential disruption to OT operations.	
B.6.7	**Advocate**	The organisation has implemented monitoring and review of the audit findings, at least quarterly to ensure that they are remediated within the stipulated timeline.	#	#	#
B.6.8		The organisation has established and implemented processes to report and follow up on the findings with the Board and/or senior management to ensure that they are informed of the audit findings and critical risks.	#	#	#

B.7 Domain: Training and awareness

This domain ensures the organisation has instilled cybersecurity awareness and culture among its employees, preventing them from becoming the weakest link in the organisation's defences.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.7.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene, under "A.1 Assets: People", to ensure that employees are equipped with the security	#	#	#

		knowledge and awareness to identify and mitigate against cyber threats.			
B.7.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under “A.1 Assets: People” to ensure that employees are equipped with the security knowledge and awareness to identify and mitigate against cyber threats.	#	#	#
B.7.3		The organisation takes measures to track the relevant metrics (e.g., attendance) to ensure that employees have completed the cybersecurity awareness and training programmes.	#	#	#
B.7.4	**Promoter**	The organisation takes measures to ensure that employees are assessed at the end of the awareness and training programmes, and are required to pass the programmes so that they demonstrate what they have learnt.	#	#	#
B.7.5		The organisation has appointed a cybersecurity champion to promote	#	#	#

		cybersecurity awareness and launch cybersecurity initiatives.			
B.7.6	**Performer**	The organisation has established and implemented policies and procedures on the training types, frequency and attendees' requirements as well as the steps to conduct and participate in the training to ensure that they can be adhered to.	#	The organisation has included cross-domain training of IT and OT teams to equip them with the skillsets to prepare for a converged IT/OT environment.	#
B.7.7		The organisation has its cybersecurity awareness and training programmes endorsed by the Board and/or senior management to ensure that they are in place and up to date.	#	#	#
B.7.8		The organisation has defined and established policies and processes to identify the cybersecurity skillsets necessary for its employees, including the Board and/or senior management, to manage cybersecurity risks and incidents, and to ensure that they receive the relevant training.	#	#	#
B.7.9	**Advocate**	The organisation has established and implemented a process to evaluate the effectiveness of the	#	#	#

		cybersecurity awareness and training programmes, e.g., by monitoring the results of trainings, the number of related cybersecurity incidents before and after the training programmes.			
B.7.10		The organisation has established and implemented a process to conduct regular skill gap analysis to identify lacking cybersecurity skillsets.	#	#	#
B.7.11		The organisation has a department (e.g., team within Human Resource (HR), business units) to be responsible for conducting, reviewing and ensuring the compliance of employees' awareness and compliance with the training programmes.	#	#	#

B.8 Domain: Asset management

This domain ensures hardware and software assets within the organisation environment are identified and tracked, enabling the implementation of cybersecurity measures and/or processes across the asset lifecycle. Active asset management allows the organisation to monitor for asset risks and control assets within its environment, ensuring only authorised assets are used and installed.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.8.1	**Supporter**	The organisation has implemented all the	#	#	#

		cybersecurity requirements in the mark of cyber hygiene under A.2 Assets: Hardware and software to ensure that hardware and software present in the environment are identified and protected against common cyber threats.			
B.8.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under A.2 Assets: Hardware and software to ensure that hardware and software present in the environment are identified and protected against common cyber threats.	#	#	#
B.8.3	**Promoter**	The organisation has established and implemented policies and procedures on the security requirements, guidelines and detailed steps to classify, handle and dispose of hardware and software assets in the environment securely to ensure that employees have clear direction and guidance.	For secure deletion and/or destruction of the organisation's data that has been stored in the cloud, as cloud services may replicate data across multiple servers and locations, the organisation has reviewed the data deletion/destruction practices practised by its CSPs, (e.g., deletion of customer data through cryptographic erasure) to ensure such practices are in alignment with its organisational policies.	#	For classification and secure handling and deletion of the organisation's data used for/in AI, the organisation has included its AI models and any training data used to train the AI models in its policies and procedures.

B.8.4		The organisation has established and implemented a process to classify and handle hardware and software according to their confidentiality and/or sensitivity levels to ensure that they receive adequate security and protection.	#	For OT, as the priority is on safety and availability, the organisation has established and implemented such classification and handling process to factor in safety and availability, e.g., security levels.	#
B.8.5		The organisation has defined and allocated roles and responsibilities to ensure that it is clear who is responsible to maintain, support and manage the hardware and software assets in the inventory list.	#	#	#
B.8.6	**Performer**	The organisation has established and implemented asset discovery tools that are appropriate and recognised in the industry to scan and discover assets that are connected to its network to ensure that all the assets can be managed securely.	The asset discovery tool implemented by the organisation has the capability to track and manage the organisation's cloud-based assets, e.g., virtual machines, containers, storage buckets, databases.	The organisation has implemented asset discovery tools that are purpose-built or tailored for OT. – Where automated scanning tools are used, the organisation has considered using passive scanning tools that are not intrusive, as active scanning can have negative impact on OT operations or safety; – Where the OT environment contains isolated systems, components, or systems	#

				connected on non-Internet Protocol (IP) networks, to complement asset discovery tools, the organisation has established and implemented manual processes to support asset discovery.	
B.8.7		The organisation has established and implemented an acceptable use policy on the rules and restrictions for hardware and software assets to ensure that the assets are being managed appropriately and securely.	#	#	#
B.8.8	**Advocate**	The organisation has established and implemented policies and process to ensure that the hardware and software asset inventory is consistent and updated organisation-wide.	#	#	#
B.8.9		The organisation has established and implemented the use of an asset inventory management system that is appropriate and recognised in the industry to track and manage hardware and software assets to ensure accuracy and avoid oversight.	The organisation's asset inventory management system has the capability to track and manage cloud assets.	The organisation's asset inventory management system has the capability to track and manage OT assets.	The organisation's asset inventory management system has the capability to track and manage AI tools, services and/or systems.

B.8.10		Asset risks are being addressed as part of the risk assessment framework and reported to the Board and/or senior management to ensure that they are not neglected.	#	#	#

B.9 Domain: Data protection and privacy

This domain ensures that business-critical data within the organisation's environment is identified and tracked, enabling the implementation of cybersecurity measures and/or processes across the asset lifecycle. It also ensures that data collection, processing, transfer and storage are secure to protect them from unauthorised access and/or disclosure.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.9.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene under "A.3 Assets: Data" to ensure that business-critical data (including personal data, company secrets, intellectual property) can be identified, located and secured.	#	#	#
B.9.2		The organisation has defined and applied a process to report any business-critical data (including personal data, company secrets, intellectual property) breach and to ensure that stakeholders such as the management, relevant	#	#	#

		authorities and relevant individuals are kept informed.			
B.9.3		The organisation using encryption has defined and applied a process on the use of recommended protocol and algorithm and minimum key length to ensure that it is secure and in alignment to industry best practices.	#	In situations where encryption has been implemented and this results in latency that has negative impact on OT operations or safety, the organisation has established and implemented reasonable compensating controls.	#
B.9.4	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under “A.3 Assets: Data” to ensure that business-critical data (including personal data, company secrets, intellectual property, etc) can be identified, located and secured.	#	#	#
B.9.5	**Promoter**	The organisation has established and implemented policies and procedures to carry out risk classification and handle business-critical data (including personal data, company secrets, intellectual property, etc) according to their confidentiality and/or sensitivity levels to ensure that they receive adequate security and protection.	#	For OT, as the priority is on safety and availability, the organisation has established and implemented such classification and handling policies and procedures to also factor in safety and availability. Examples of OT data include controller configuration files, Programmable Logic Controller (PLC) program	The organisation has established and implemented classification and handling policies and procedures for employees to identify the data sets in the organisation that could be used in both internal and external AI tools and/or services, e.g. generative AI.

				codes and computer-aided drafting/computer-aided manufacturing files.	
B.9.6		The organisation has established and implemented policies and procedures to document the data flow diagram of business-critical data (including personal data, company secrets, intellectual property) through information systems and programs in the organisation and implement relevant enforcement measures to ensure that they stay within the environment.	The organisation's data flow diagram has included data that is processed and stored in the cloud, and the geographic location(s) of data in the cloud.	The organisation's data flow diagram for OT has included the expected operational flow of data in the OT environment, including: – data flow crossing network boundaries, indicating communication channels between logical and/or physical segments; and – instances of data flow through insecure protocols.	The organisation's data flow diagram for AI has included documentation of data associated with its AI system(s), e.g.: – data used for training AI system(s) (where relevant); – data input to AI system(s); including prompts, and – data output from AI system(s).
B.9.7		The organisation has established and implemented policies and procedures to handle business-critical data (including personal data, company secrets, intellectual property, etc) securely and to protect business-critical data according to their classifications and requirements (e.g., collect, use, protect, dispose).	#	#	The organisation has implemented secure handling of: – data input to AI systems; – data models (where relevant); and – data output from AI systems. Examples of secure handling of data input to AI systems include measures for: – data integrity; – data provenance; – data validation and/or sanitisation; and

					– protection on the query interface to detect and mitigate attempts to access, modify and exfiltrate data, e.g. guardrails, rate limiting of queries. Examples of secure handling of AI models include measures for: – verification of models with hashes/ signatures; and – security evaluation of the AI systems before deployment, e.g. benchmarking, security testing, red teaming. Examples of secure handling of data output from AI systems include measures for: – verification of integrity of data output; and – generating output that is usable to users whilst not revealing unnecessary information to potential attackers.
B.9.8	**Performer**	The organisation has established and implemented data management policies and procedures through the	The organisation's data management policies and procedures has taken into consideration:	#	#

		guidelines, requirements and steps to handle business-critical data (including personal data, company secrets, intellectual property) at rest, in transit and in use, securely.	– the ability to maintain oversight of where data in the cloud is stored, processed, and backed up to ensure it is in line with organisation's obligations; and – The ability to manage migration of data securely between cloud environments for interoperability and portability.		
B.9.9		The organisation has defined and allocated roles and responsibilities to ensure that it is clear who is responsible to maintain, support and manage the data assets in the inventory list.	#	#	#
B.9.10	**Advocate**	The organisation uses encryption to protect its data and has established and implemented cryptographic policies and processes to ensure that the keys are being handled securely throughout the cryptography key management lifecycle.	The organisation has incorporated best practices for cryptography into its policies and processes. Examples include: – secure storage and use of API keys, secrets, passwords, secure shell (SSH) keys, or certificates, e.g., secure procedure for key lifecycle	#	For sensitive data, the organisation has considered the use of privacy-preserving techniques, e.g., anonymisation, differential privacy (where applicable) for data protection.

			from generation to revocation; and – regular scanning to search for static credentials and keys/secrets stored in cleartexts. The organisation has also considered different approaches for management of encryption keys to balance between maintaining control over the keys and leveraging a fully managed cloud service: – encryption keys managed by the CSP; – customer-managed encryption keys; and – customer-supplied encryption keys (or "bring your own key").		
B.9.11		The organisation has established and implemented policies and procedures allowing only authorised devices with secure protocols to communicate, store and transfer business-critical data (including personal data, company secrets, intellectual property) within the organisation.	Examples include Data Security Posture Management (DSPM) solutions or equivalents to protect sensitive data and support compliance with data protection regulations within cloud environments.	In situations where the OT environment uses authorised devices that support insecure protocol(s), the organisation has established and implemented reasonable compensating controls.	#

B.9.12		The organisation has established and implemented policies and procedures to report on data protection and privacy risks and initiatives to the Board and/or senior management to ensure that they are kept informed.	#	#	#

B.10 Domain: Backups

This domain ensures that information assets are regularly backed up in a secure and consistent manner so that the organisation can restore and recover its systems and data in the event of a cybersecurity and/or breach of data incident.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.10.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene under “A.8 Backup: Back up essential data” to ensure that the organisation’s essential data is backed up and stored securely.	#	#	#
B.10.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under “A.8 Backup: Back up essential data” to ensure that the	#	#	#

		organisation's essential data is backed up and stored securely.			
B.10.3		The organisation has established and implemented automated backup processes to ensure that the backup tasks are carried out without fail and without the need for human intervention.	In its automated backup process, the organisation has included backups of its cloud services.	In situations where automated backup is not appropriate or recommended, e.g., has a negative impact on OT operations or safety, the organisation has established and implemented regular scheduled backups to be performed manually.	
B.10.4	**Promoter**	The organisation has established and implemented backup plan(s) on the types, frequency and storage of backups to ensure that there is clarity of the steps to be taken to backup business-critical data in the organisation.	#	For OT, as the priority is on safety and availability, the organisation has considered the use of immutable storage for critical OT data, which may include programs or device configurations, as such storage provides: – additional data integrity through data storage in a read-only format; and – added protection against the installation of new software when used as a read-only drive in a maintenance workstation.	#
B.10.5		The organisation has established and implemented the use of technology solutions for data backup and recovery, and the solutions implemented are appropriate and recognised	#	#	#

		in the industry to ensure that it can carry out reliable data backup and restoration.			
B.10.6	**Performer**	The organisation has established and implemented backup and recovery policies and procedures on the requirements, guidelines and detailed steps to ensure that there is consistent guidance and direction for performing backup and recovery in the organisation.	The organisation has implemented the appropriate backup and recovery policies and procedures based on the cloud shared responsibility model with its CSP. In situations where the CSP is responsible, the organisation has reviewed the backup and recovery practices of its CSPs to ensure the implementation is in alignment with its organisational policies.	#	#
B.10.7		The organisation has defined and allocated roles and responsibilities to ensure that it is clear who is responsible and accountable to perform and manage backups from creation to destruction.	#	#	#
B.10.8	**Advocate**	The organisation has established and implemented a backup control sheet for the backup data storage media with the purpose of including backup, time of backup, data encryption, retention date and the employee(s) assigned the task of backup to ensure that	#	#	#

		all the key information are documented.			
B.10.9		The organisation has established and implemented policies and procedures to report backup-related matters to the cybersecurity committees/forums to ensure that senior management is kept informed.	#	#	#
B.10.10		The organisation has established and implemented policies and procedures to perform reviews on the backup status regularly to ensure that failed backup jobs are addressed and remediated.	#	#	#

B.11 Domain: Bring your own device (BYOD)

This domain ensures that the use of personal devices is managed securely when connected to the organisation's network. This domain also addresses processes to prevent the disclosure and loss of the organisation's business-critical data through personal devices.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.11.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should consider the cybersecurity requirements in the mark of cyber hygiene under:	#	#	#

		– A.2 Assets: Hardware and software; – A.4 Secure/Protect: Virus and malware protection; – A.6 Secure/Protect: Secure configuration; – A.7 Update: Software updates; and – A.8 Backup: Back up essential data covering mobile devices.			
B.11.2	**Practitioner**	Domain is not assessable for this tier. However, the organisation should consider the cybersecurity requirements in the mark of cyber hygiene under: – A.2 Assets: Hardware and software; – A.4 Secure/Protect: Virus and malware protection; – A.6 Secure/Protect: Secure configuration; – A.7 Update: Software updates; and – A.8 Backup: Back up essential data covering mobile devices.	#	#	#
B.11.3	**Promoter**	The organisation has established and implemented policies and procedures to segregate personal and work-related data in the organisation within BYOD to prevent disclosure and loss of	#	#	#

		confidential and/or sensitive data.			
B.11.4	**Performer**	The organisation has established and implemented policies and procedures on the guidelines, requirements and steps on the use of BYOD connecting to the organisation's network and accessing the organisation's data to ensure that they conform to the set of security standards, e.g., passcode enabled.	#	#	#
B.11.5		The organisation has implemented regular review on the use of BYOD accessing business-critical data at least annually to ensure that the devices are compliant and safe.	#	#	#
B.11.6	**Advocate**	The organisation has established and implemented cybersecurity measures within BYOD to manage and enforce organisational security protection, such as through the use of mobile device management (MDM).	#	#	#

B.12 Domain: System security

This domain ensures that cybersecurity measures and safeguards are implemented and maintained to secure the organisation's systems. These measures and safeguards include secure configuration, logging, updates and patching.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.12.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene under "A.6 Secure/Protect: Secure configuration" and "A.7 Update: Software updates" to ensure that the hardware and software use secure and updated settings.	#	#	#
B.12.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under "A.6 Secure/Protect: Secure configuration" and "A.7 Update: Software updates" to ensure that the hardware and software use secure and updated settings.	#	#	#
B.12.3		The organisation has performed monitoring on updates and patches installed to ensure that any impact or adverse effects can be identified and rectified promptly.	#	#	#

B.12.4	**Promoter**	The organisation has defined and applied a process to ensure secure configurations are applied across all systems, servers, operating systems and network devices.	#	#	As part of secure configuration, the organisation has considered AI model complexity and the appropriateness of the model for the intended use case, as complex models may involve additional software packages or libraries, which expand the attack surface.
B.12.5		The organisation has defined and applied a log management process to store and classify the different types of logs securely to ensure that they can be used to troubleshoot effectively.	#	As OT devices may have limited disk space and memory, the organisation has implemented: – adequate local or remote storage to reduce the likelihood of exceeding device capacity and loss of logging capability; or – mechanisms to securely transfer and store logs from the OT devices to alternate storage.	#
B.12.6		The organisation has defined and applied a patch management process to test and install the updates and patches securely to ensure that there are no adverse effects.	#	The patch management process has taken into consideration the different availability requirements that OT sub-systems and/or network segments may have, and their corresponding differences in abilities to	#

				support patching, and the organisation has tracked the key vulnerabilities that need to be addressed.	
B.12.7	**Performer**	The organisation has defined and allocated the roles and responsibilities to oversee, manage and monitor the organisation's system security (i.e., secure configuration, logging, update and patching) to ensure that employees are clear on the tasks assigned to them.	#	#	#
B.12.8		The organisation has established and implemented policies and procedures on the security configuration requirements, guidelines and detailed steps to ensure that they are aligned with the security standards.	The organisation's policies and procedures on secure configuration for cloud workloads have incorporated best practices. Examples for IaaS or PaaS users include: – images for containers or virtual machines: ▪ use of images from trusted sources only; ▪ use of automated, centrally managed, versioned and immutable base images for deployment; ▪ verification of image integrity to detect	#	The organisation's policies and procedures on secure configuration for AI have incorporated best practices. Examples include: – model hardening, e.g., through adversarial training; – prompt engineering best practices including use of guardrails; – monitoring and limiting the rate of queries to AI systems; or – use of ensembles of models for better

			unauthorised modifications, keeping images up-to-date with the most recent security patches; – virtual machine security: ▪ use of configuration management or Infrastructure as Code (IaC) to mitigate configuration drift; ▪ hardening of configuration on virtual machine instances; and – container orchestration security: hardening of orchestration services.		resilience against attacks.
B.12.9		The organisation has established and implemented a secure logging policy and procedure with the requirements, guidelines and detailed steps to store, retain and delete the logs from unauthorised access.	This includes a secure logging policy and procedure for the organisation's cloud workloads. Examples for IaaS and PaaS users include logging of: – containers or virtual machines for unusual behaviour; and – user interactions.	#	#
B.12.10		The organisation has established and implemented policies and procedures with the requirements, guidelines and detailed steps to perform	The organisation has implemented the appropriate patch management policies and procedures based on the	#	#

		and install patches/updates to ensure that the system(s) is/are patched or updated within the defined timeframes according to their priority.	cloud shared responsibility model with its CSP. In situations where the CSP is responsible, the organisation has reviewed the patch management practices of its CSPs, to ensure the implementation is in alignment with its organisational policies.		
B.12.11	**Advocate**	The organisation has implemented a configuration management tool/solution that is appropriate and recognised in the industry to ensure that the system's configurations are maintained in a desired and consistent state.	The organisation has implemented solutions such as cloud-native tools for cloud configuration management, e.g. cloud security posture management (CSPM) solution, cloud-native application protection platform (CNAPP) or equivalent, to support configuration management of cloud workloads.	The organisation has implemented configuration management tool/solutions that can manage OT configuration information, where feasible.	#
B.12.12		The organisation has established and implemented policies and procedures to ensure that the system's configuration requirements are aligned with the industry benchmarks and standards. NOTE – An organisation that offers system configuration	#	For specialised OT systems, the organisation has obtained these configuration requirements from its OT vendors and/or service providers.	#

		benchmarks is the Center for Internet Security (CIS).			
B.12.13		The organisation has established and implemented policies and procedures to ensure that the systems' configurations are being complied and the risks as a result of non-compliance are being addressed.	#	#	#

B.13 Domain: Virus and malware protection

This domain ensures that protection measures and technologies are implemented, maintained, and updated to continuously monitor and defend against malware, which may disrupt or damage the network. This domain also addresses the processes implemented to manage successful malware attacks, so that further damage and spread to the network and environment is prevented.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.13.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene under "A.4 Secure/Protect: Virus and malware protection" to ensure that there is security protection against malicious software such as virus.	#	#	#
B.13.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark	#	#	#

		of cyber hygiene under “A.4 Secure/Protect: Virus and malware protection” to ensure that there is security protection against malicious software such as virus.			
B.13.3		The organisation has established and implemented the use of virus and malware protection solution(s) that is/are appropriate and recognised in the industry with features such as real-time malware detection and email protection e.g., DMARC, to ensure that it/they can protect the organisation adequately.	The organisation has implemented the appropriate virus and malware protection based on the cloud shared responsibility model with its CSP. In situations where the CSP is responsible, the organisation has reviewed the virus and malware protection practices of its CSPs, to ensure the implementation is in alignment with its organisational policies.	#	#
B.13.4		The organisation has established and implemented web filtering to protect the organisation from malicious websites.	#	#	#
B.13.5		The organisation has defined and applied the process to isolate and contain the virus and/or malware upon confirmation of attack to ensure minimal spread and damage caused.	The organisation has developed a process for the removal of malware that has been detected in the organisation’s cloud environment, in accordance with applicable contractual	#	#

			agreements with its CSPs and its own organisational policies.		
B.13.6	**Promoter**	The organisation has defined and applied the process to run codes or applications of unknown origin within an isolated testing environment to test for the presence of virus and/or malware prior to their use in the working environment.	#	The organisation has implemented processes such that codes or applications of unknown origin are not implemented in the OT environment. In situations where new updates are released by authorised vendors, and the organisation does not have redundant or spare equipment or systems to support such testing, the organisation has made arrangements to conduct such testing within the vendor's test environment, or performed testing on its own setup during scheduled maintenance windows or downtime.	#
B.13.7	**Performer**	The organisation has defined and allocated the roles and responsibilities for employees to oversee, manage and maintain the virus and malware protection solution(s) to ensure clarity for the relevant employees of their required tasks.	#	#	#

B.13.8	**Advocate**	The organisation has established and implemented policies and processes to subscribe to threat intelligence from external parties and to share and verify information relating to cyberattacks, which includes virus and/or malware attacks.	The organisation has established and implemented policies and processes to maintain visibility of cloud-specific threats, including adversaries targeting the cloud-based environment, e.g., subscribing to threat intelligence which include cloud-based threats, participation in cloud-related special interest groups or equivalent, to receive early warnings and advice regarding new threats and vulnerabilities.	The organisation has established and implemented policies and processes to maintain visibility of OT-specific threats, e.g., subscribing to OT-specific threat intelligence, including that tailored for its own or adjacent sectors, participating in OT-specific special interest groups or equivalent, to receive early warnings and advice regarding new threats and vulnerabilities.	The organisation has established and implemented policies and processes to maintain visibility of AI-specific threats, including adversaries targeting AI, e.g., subscribing to threat intelligence which include AI-specific threats, participation in AI-related special interest groups or equivalent, to receive early warnings and advice regarding new threats and vulnerabilities.
B.13.9		The organisation has established and implemented policies and processes to review and report findings on virus and/or malware to the Board and/or senior management to ensure that they are kept informed.	#	#	#
B.13.10		The organisation has established and implemented scanning and detection of indicators of compromise to ensure early identification of anomalies and suspicious activities.	#	#	#

B.14 Domain: Secure Software Development Life Cycle (SDLC)

This domain ensures that security specifications and practices are incorporated into the system's SDLC so that the software can be developed in a secure and consistent manner.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.14.1	**Supporter**	Domain is not assessable for this tier.	#	#	#
B.14.2	**Practitioner**	Domain is not assessable for this tier.	#	#	#
B.14.3	**Promoter**	The organisation has established and implemented security guidelines and requirements in its system and/or application development. Examples include: – secure coding; – secure management of API keys; – reviewing the security posture of third-party software, including open source; and – adhering to best practices and/or standards to ensure that it adheres to the security principles.	Examples include: – securing APIs used for accessing and configuring cloud resources and data (e.g., implementing authentication and authorisation), as APIs exposed on public-facing assets in the cloud increase the attack surface and are priority targets for malicious actors; – securing the information being transferred between the API and the applications that interface with it using encryption and/or security protocols; – performing input verification of data being relayed to an API as a	#	These security guidelines and requirements have been established and implemented across the life cycle of the organisation's AI systems, i.e.: – design; – development; – deployment; and – operations and maintenance.

		NOTE – In Singapore, the Safe App Standard provides guidance on implementing essential security controls and best practices for mobile app development.	safeguard against attacks such as structured query language (SQL) injection, cross-site scripting (XSS), potential execution of remote code; – deploying a web application firewall to block malicious API requests; – implementing rate limiting to restrict the number of API requests within a specified period to prevent brute-force attacks and other malicious behaviour; – enabling logging and monitoring on API traffic to identify anomalies or possible security threats; and – using DevSecOps to automate core security tasks by embedding security checks, scans, and tests into the continuous integration and continuous delivery (CI/CD) workflow to facilitate rapid and secure delivery of code changes.		
B.14.4	**Performer**	The organisation has established and implemented an SDLC framework with cybersecurity measures and	The organisation has implemented relevant SDLC frameworks for cloud, e.g.:	The organisation has implemented relevant SDLC frameworks for OT, e.g.: – security management;	The organisation has implemented relevant SDLC frameworks for AI, e.g.:

		requirements to manage the software development life cycle ensuring that areas such as data integrity, authentication, authorisation, accountability and exception handling can be addressed.	– secure design and architecture; – secure coding – continuous build, integration, and testing; – continuous delivery and deployment; and – runtime defence and monitoring.	– specification of security requirements; – security by design; – secure implementation; – secure requirements testing; – security update management; and – security guidelines.	– secure design; – secure development; – secure deployment; and – secure operations and maintenance.
B.14.5	**Advocate**	The organisation has established and implemented the change management policy and process to ensure that changes or deployments to the production environment are reviewed and tested securely, with a rollback plan in place to ensure that the change is controlled.	#	#	#
B.14.6		The organisation has established and implemented a policy and process to perform security testing on the system and/or application before deployment to identify security weaknesses and vulnerabilities.	#	#	This has included security testing on the organisation's AI system(s), e.g., adversarial testing.

B.15 Domain: Access control

This domain ensures that sufficient access management controls and formalised processes are in place so that the access to the organisation’s assets and data by employees, contractors and third parties are granted only on a least privilege basis and managed in a controlled and consistent manner.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.15.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene under “A.5 Secure/Protect: Access control” to ensure that there are cybersecurity measures in place over who has access to the data and assets.	#	#	#
B.15.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under “A.5 Secure/Protect: Access control” to ensure that there are cybersecurity measures in place over who has access to the data and assets.	#	#	#
B.15.3		The organisation performs regular role matrix review at least on an annual basis on the systems to ensure that the roles commensurate with the activities the employee, contractor and/or third party is allowed to perform.	#	#	#
B.15.4	**Promoter**	The organisation has defined and implemented a process to approve and follow up on	#	#	#

		account access and role matrix reviews to ensure that unauthorised entry is rectified and signed off.			
B.15.5		The organisation has defined and applied a process to ensure that employees are assigned roles based on the principle of least privilege and segregation of duties.	In addition to roles for employees, for organisations using IaaS or PaaS, the organisation has also implemented the principle of least privilege for cloud workloads by granting them the minimum permissions necessary to perform their assigned tasks and reviewing the permissions of the workloads to ensure that they do not have excessive permissions.	#	#
B.15.6		The organisation has established and implemented a secure log-on policy and procedure outlining the requirements, guidelines and detailed steps for gaining access to sensitive and/or business-critical data, as well as privileged access to ensure that the access is controlled and restricted.	Examples of a secure log-on policy and procedure include: – implementing protection of its cloud management plane (e.g. CSP console) access and activity; – implementing measures to enable the organisation to scale the management of users and identities for cloud computing, e.g., identity federation; – implementing authorisation measures that allow more granular control, e.g., use of	The organisation has implemented separate authentication mechanisms and/or credentials for employees that have access to both OT and IT (or corporate) networks to mitigate against lateral movement between corporate IT networks and the OT environment in the event that employee credentials are compromised. For OT, as the priority is on safety and availability,	#

			attribute-based access control (ABAC) or policy-based access control (PBAC) to complement role-based access control (RBAC), where access is granted to all users with a given role, where available and feasible; – eliminating the use of static cloud credentials such as hard-coded API keys where feasible; and – using temporary access tokens instead of permanent/static credentials/permissions for data sharing with external parties.	the organisation has taken into consideration how any potential delay associated with the secure logon policy and procedures has not impeded access of OT personnel in emergency situations.	
B.15.7	**Performer**	The organisation has established and implemented a passphrase policy and procedure outlining the requirements, guidelines and detailed steps on setting and updating passphrases to provide guidance and direction on what constitutes strong passphrases.	#	The policy and procedure have outlined the respective limitations and the corresponding compensating controls for OT assets where: – default passwords cannot be changed; – secure passwords or passphrases are not supported; – passwords or passphrases are transmitted in cleartext due to legacy protocols; – passwords are not recommended; or	#

				– other limitations or constraints exist.	
B.15.8		The organisation has established and implemented a user access control policy and procedure outlining the requirements, guidelines and detailed steps to restrict and authorise users' access to its assets.	#	#	#
B.15.9		The organisation has established and implemented secure remote access policies and procedures outlining the requirements, guidelines and detailed steps to protect information accessed remotely.	#	#	#
B.15.10	**Advocate**	The organisation has established and implemented policies and processes to review any signs of access compromise and to report the results to the Board and/or senior management to ensure that they are kept informed.	#	#	#
B.15.11		The organisation has established and implemented a privileged access solution that is appropriate and recognised in the industry to authenticate users and authorise access based on their roles to ensure that there is a more efficient	To implement privileged access for the cloud environment, the organisation has implemented measures to scale the management of cloud identities and their entitlements to mitigate the	The organisation has implemented separate deployments of privileged access solutions to manage privileged access for the OT and IT environment respectively, to mitigate against lateral movement	#

		and effective way of managing access.	risk of unauthorised access and data breaches, e.g., using identity providers to authenticate users through SSO, use of cloud identity and entitlement management (CIEM) solutions, cloud-based identity and access management (IAM), CNAPP, or equivalent.	between corporate IT networks and the OT environment, should privileged access credentials be compromised.	

B.16 Domain: Cyber threat management

This domain ensures that the organisation actively identifies threats and security anomalies within their operating environment, across systems, network devices and employees, so that early detection and response activities can be carried out.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.16.1	**Supporter**	Domain is not assessable for this tier.	#	#	#
B.16.2	**Practitioner**	Domain is not assessable for this tier. However, the organisation should ensure that logging is enabled for software and hardware assets, e.g., systems, events, security and debugging logs.	#	#	#
B.16.3	**Promoter**	Domain is not assessable for this tier. However, the organisation shall ensure that logging is enabled for software and hardware assets, e.g.,	#	#	#

		systems, events, security and debugging logs.			
B.16.4	**Performer**	The organisation has established and implemented a log monitoring policy, process and procedure outlining the requirements, guidelines and detailed steps for monitoring security logs for threats and abnormalities.	The organisation has incorporated cloud best practices for its log monitoring policy, process and procedure. Examples include: – verifying that CSPs provide adequate logging capabilities, e.g., access to logs, retention period of logs, to ensure alignment with organisational policies; – prioritising logs for cloud workloads that may be most indicative of security issues, such as logs from the management plane, identity and access management activity, or changes in public-facing resources; – automating log retrieval from CSPs; – normalising cloud logs to a common format across cloud applications to facilitate log analysis; and – normalising event, audit, activity, and other log entries that include user information (such as	#	The log monitoring policy, process and procedure have included: – monitoring inputs to the AI models or AI systems for possible attacks and suspicious activity; and – monitoring AI model or system outputs and performance.

			usernames) to a corporate identity so that events that refer to the same person in different usernames/user accounts in different cloud applications can be correlated.		
B.16.5		The organisation has defined and assigned roles and responsibilities to carry out log monitoring and reviews of its systems, investigate incidents and report to relevant stakeholders.	#	The organisation has assigned roles and responsibilities to monitor and review logs, and investigate and report incidents for both OT and IT as OT and IT security operations converge, and OT and IT teams may be distinct and operate independently.	#
B.16.6		The organisation has implemented security information and event management (SIEM) to store logs centrally for correlation and to ensure more effective log monitoring.	The organisation's SIEM implementation has the capability to manage logs for the organisation's cloud workloads.	In situations where active scanning by the SIEM solution is not appropriate or recommended in the OT environment, the organisation has: – implemented passive scanning; or – performed active scans during scheduled maintenance windows or downtime.	#
B.16.7		The organisation has established and implemented a security baseline profile on its systems to analyse and	#	Recognising that the OT environment has a deterministic nature and OT activities and traffic tend to be more predictable and	#

		perform monitoring to ensure that anomalies are identified.		repeatable, the organisation has established a baseline of normal network traffic and data flows that factors in normal human and OT process behaviour, to differentiate between normal or transient conditions and anomalies and minimise false positive alerts.	
B.16.8		The organisation has established and implemented policies and procedures on the requirements, guidelines and detailed steps to be carried out when it detects abnormal or suspicious logs, to ensure that they are investigated, reported and remediated promptly.	#	For OT, because the priority is safety and availability, the organisation's policies and procedures have indicated its response priority, e.g., restoring OT operations to normal versus performing investigation and preserving forensic data.	#
B.16.9	**Advocate**	The organisation has established and implemented advanced analytics processes and solutions that are appropriate and recognised in the industry to detect abnormal system and user behaviour, e.g., user behaviour analytics.	#	#	#
B.16.10		The organisation has established and implemented reporting requirements and dashboards to report detected cybersecurity incidents or anomalies based on their	#	#	#

		severity to the Board and/or senior management.			
B.16.11		The organisation has established and implemented measures and processes to proactively search for threats that are hidden in its IT environment.	This includes threat hunting in the organisation's cloud environment.	This includes threat hunting for hidden threats targeting the OT environment, the organisation's own sector or adjacent sectors.	This includes measures such as performing red teaming on the organisation's AI systems.

B.17 Domain: Third-party risk and oversight

This domain ensures that sufficient cybersecurity measures and/or processes are established to manage third-party risks so that the organisation can minimise and control the risks caused by services provided by third-party service providers.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.17.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should ensure that requirements on third parties in the mark of cyber hygiene under – "A.2 Assets: Hardware and Software" – "A.3. Assets: Data" – "A.5 Secure/Protect: Access control"; and – "A.6 Secure/Protect: Secure configuration" have been implemented.	#	#	#

B.17.2	**Practitioner**	Domain is not assessable for this tier. However, the organisation should ensure that requirements on third parties in the mark of cyber hygiene under – "A.2 Assets: Hardware and Software" – "A.3 Assets: Data" – "A.5 Secure/Protect: Access control"; and – "A.6 Secure/Protect: Secure configuration" have been implemented.	#	#	#
B.17.3	**Promoter**	The organisation has established and implemented service-level agreements with its third parties to ensure that the third party meets the commitments and expectations on cybersecurity while providing services.	The service level agreement with the organisation's CSPs has incorporated key areas related to cloud security. Examples include: – performance metrics of cloud services and resources, e.g., availability; – information security requirements (including shared cloud responsibility model); – change management process, e.g.; software updates;	#	The service level agreement with the organisation's AI suppliers has incorporated key areas related to AI security. Examples include: – performance metrics of AI services, e.g. availability; – information security requirements, including responsibility of supplier for security; – guardrails and other measures implemented for security;

			– logging and monitoring practices, e.g., log and data retention period; – incident management and communications procedures, e.g., support hours, maximum first support response time; – attainment of cloud security standards; and – data privacy.		– change management process, e.g., software updates; – logging and monitoring practices; – incident management practices; and – use of the organisation's data for training of the supplier's AI models.
B.17.4	**Performer**	The organisation has established and implemented measures to ensure that minimum cybersecurity requirements are defined for third parties, and that third parties are informed of their security obligations and to ensure that security is established for systems and data.	This has included establishing a shared responsibility model with the organisation's CSPs (and data centre service providers, where relevant), including a review of the following practices: – Notification to the organisation within a specific timeframe if the CSP identifies a vulnerability for which the organisation can apply compensating controls to reduce its severity or likelihood of exploitation; and – Support from the CSP for resolving or mitigating vulnerabilities in the CSP's services.	This has included reviewing the practices of the organisation's third parties for OT in situations where there is heavy reliance on the OT supply chain, e.g., OT vendors: – cybersecurity posture of third parties' products, services and/or systems; and – cybersecurity practices of third parties when supporting the organisation in providing software upgrades and patches, performing integration services, or supporting the operations and maintenance of OT systems.	This has included establishing a security shared responsibility model for AI with the organisation's AI providers, where feasible, to cover: – the security areas for which the organisation is responsible, including its responsibility to meet its customers' expectations and needs; and – the security areas for which its suppliers and/or third-party partners are responsible.

B.17.5		The organisation has established and implemented measures to assess its third parties before engaging them or onboarding them to ensure that they meet all required security obligations based on the risks for the type of services provided.	This has included an assessment of the minimum cybersecurity requirements to be met by: – its CSPs; and – third-party software and images used by the organisation in the cloud, including open source, based on the risk level of the project.	This has included an assessment of the minimum cybersecurity requirements to be met by its third parties, based on the risk level of the project.	This has included an assessment of the minimum cybersecurity requirements to be met by its third parties based on the risk level of the project – For external model providers: Due diligence evaluation of the provider's own security posture. – For external software libraries, including open source: Due diligence evaluation of the libraries, e.g., AI code checking, vulnerability scanning, or checking against a database with vulnerability information. – For external APIs: Implementation of controls on data that is sent to services outside of the organisation, e.g., requiring users to log in to confirm before sending potentially sensitive information. Where there is use of models or code that is not from trusted sources, the

					organisation has implemented appropriate controls, e.g. sandboxing.
B.17.6	**Advocate**	The organisation has established and implemented measures to assess their third parties regularly based on agreed-upon security obligations for systems security and data protection.	#	#	#
B.17.7		The organisation has established and implemented measures to ensure that third-party cybersecurity risk management practices, such as assessments performed and open risks from third parties engaged, are reported to the Board and/or senior management to keep them informed.	#	#	#

B.18 Domain: Vulnerability assessment

This domain ensures that vulnerability assessment and management are established to keep the organisation's network and systems safe from known exploitation. This domain also ensures processes are established to identify, evaluate, mitigate, and report on security vulnerabilities in systems and the software.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.18.1	**Supporter**	Domain is not assessable for this tier.	#	#	#

B.18.2	**Practitioner**	Domain is not assessable for this tier.	#	#	#
B.18.3	**Promoter**	The organisation has established a vulnerability assessment plan with objectives, scope and requirements to review and perform vulnerability assessments on its systems.	The vulnerability assessment plan has included the organisation's cloud environment.	The vulnerability assessment plan has included identification and evaluation of the threats and vulnerabilities within each OT sub-system and/or network segment and/or zone.	#
B.18.4		The organisation performs regular vulnerability assessments, at least annually, to conduct non-intrusive scans on its systems to ensure that vulnerabilities are discovered.	The vulnerability assessment has included the organisation's cloud environment. Examples include the following: – Images: Building vulnerability assessment agents into images. – Virtual machines: Performing runtime vulnerability assessment/scans by taking snapshots of virtual machines and assessing them offline, without affecting the running workload.	When conducting vulnerability assessments, where active scanning could interfere with real-time OT operation, the organisation has considered passive scanning and monitoring tools that are not intrusive to OT systems. If active scanning is performed, the organisation has included, in its vulnerability assessment plan, a process for testing to be conducted first, and to perform such scans during scheduled maintenance windows or downtime.	The vulnerability assessment has included the organisation's AI systems.
B.18.5	**Performer**	The organisation has defined and allocated roles and responsibilities for its employees on carrying out	#	#	#

		cybersecurity vulnerability assessment and management.			
B.18.6		The organisation has established and implemented policies and procedures outlining the requirements, guidelines and detailed steps for conducting cybersecurity vulnerability assessments across its systems to ensure that steps are taken to address the associated risk vulnerabilities identified promptly.	The vulnerability assessment policy and procedure have included the organisation's cloud environment. The organisation has verified that the vulnerability assessment policy and procedure is in alignment to the CSP's support policy for vulnerability assessment.	#	#
B.18.7		The organisation has established and implemented measures and processes to track, review, evaluate and address the vulnerabilities uncovered as part of the assessments to ensure that the vulnerabilities are remediated according to their severity.	#	In situations where vulnerabilities cannot be mitigated promptly (e.g., legacy OT devices or systems where software patches are not available, the organisation has implemented compensating controls to address these vulnerabilities.	#
B.18.8	**Advocate**	The organisation has established and implemented a penetration test plan with the objectives, scope and rules of engagement to ensure that the penetration test can be performed safely.	The penetration test plan has included the organisation's cloud environment. The organisation has verified that the penetration test plan is in alignment to the CSP's support policy for penetration testing.	The organisation's test plan for penetration testing for the OT environment has: – implemented measures to ensure that OT functions are not adversely impacted by the testing process as OT systems can be highly sensitive to timing	#

				constraints or operate with limited resources; – factored in the use of compensating controls, such as employing a replicated, virtualised, or simulated system to conduct penetration testing where relevant; and – factored in the need to take production OT offline, during scheduled maintenance windows or downtime, before testing can be conducted where relevant.	
B.18.9		The organisation performs regular penetration tests, at least annually, to discover and exploit security weaknesses in its systems to ensure that its system's security can be evaluated.	#	#	#
B.18.10		The organisation has established and implemented metrics and thresholds, including dashboards, to provide reporting and tracking of open, overdue and severe vulnerabilities noted within its systems to provide visibility on tracking and remediations within established timelines.	#	#	#

B.18.11		The organisation has established and implemented practices and measures to regularly report on the vulnerability assessment results and findings to the Board and/or senior management.	#	#	#

B.19 Domain: Physical/environmental security

This domain ensures that physical/environmental security measures are established to protect people, property, and physical assets. This domain also ensures a process is implemented to monitor and report physical/environmental risks and controls.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.19.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cultivating cybersecurity leadership in the organisation, educating employees on cybersecurity, securing access and	#	#	#

		environment and protecting your information assets.			
B.19.2	**Practitioner**	The organisation has identified the physical/environmental risks in its environment and implemented detective measures to be alerted to threats to ensure that they are addressed promptly.	#	Examples include: – physical access of unauthorised personnel to the OT environment; and – natural disasters or power outages that disrupt the organisation's cybersecurity practices, rendering its OT environment vulnerable to cybersecurity incidents.	#
B.19.3		The organisation has taken measures to protect its physical assets against internal and external threats, e.g., using cable locks to prevent theft or tampering.	#	As logical and/or physical segmentation is used to characterise or isolate OT assets based on their risk or criticality levels or security requirements, the organisation has implemented physical controls for isolating OT sub-systems and/or network segments, e.g., use of locked cabinets or rooms to house OT assets.	#
B.19.4		The organisation has implemented physical security measures on its perimeters, e.g., fences and gates, to deter unauthorised access to the premises.	The organisation has verified that the physical security measures implemented by its CSPs, e.g., providers' statements on physical security controls, including their data centres, certification(s) of recognised	#	#

			and appropriate standards that cover physical security, are in alignment with its requirements.		
B.19.5	**Promoter**	The organisation has defined and implemented a process to ensure that visitors are registered and authorised before accessing the premises.	#	#	#
B.19.6		The organisation has defined and implemented a process to monitor its premises 24/7, e.g., using CCTV, to deter and investigate physical/ environmental threats.	#	#	#
B.19.7		The organisation has defined and applied a process to store and transport physical media containing business-critical data securely within and outside its premises to ensure that confidential and/or sensitive data are protected.	#	#	#
B.19.8	**Performer**	The organisation has established and implemented policies and procedures outlining the requirements, guidelines and detailed steps for escalation and security access controls to minimise the impact and interference to its physical environment.	#	#	#

B.19.9		The organisation has defined and assigned roles and responsibilities for detecting, mitigating and responding against physical/environmental risks to ensure that employees understand their assigned tasks.	#	#	#
B.19.10		The organisation has established and implemented policies and procedures outlining the requirements, guidelines and detailed steps to review physical security measures and assets to ensure that they remain secure.	#	#	#
B.19.11	**Advocate**	The organisation has established and implemented policies or processes to report physical/environmental risks and controls to the Board and/or senior management to ensure that they are kept informed of the risks.	#	#	#
B.19.12		The organisation has established and implemented a process to review and improve the physical/environmental security measures to ensure that they are effective.	#	#	#

B.20 Domain: Network security

This domain ensures that sufficient cybersecurity measures and/or processes to secure the confidentiality and accessibility of the organisation's network and data are established.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.20.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should ensure requirements on network security in the mark of cyber hygiene under – "A.2 Assets: Hardware and Software"; – "A.4 Secure/Protect: Virus and malware protection"; and – "A.6 Secure/Protect: Secure configuration" have been implemented.	#	#	#
B.20.2	**Practitioner**	The organisation has configured and implemented access controls, e.g., whitelisting, blacklisting, on its network to enforce network security policy and ensure that unauthorised users and/or devices are kept out.	#	#	#
B.20.3		The organisation has established and implemented the use of stateful firewall over	Examples include measures such as:	The organisation has implemented a firewall that is purpose-built for OT or tailored	#

		a basic packet-filtering firewall to ensure that packets are filtered with more context for greater effectiveness.	– implementing runtime protection for containers or virtual machines, e.g., network segmentation for containers or virtual machines; and – using container firewalls or virtual firewalls to manage network traffic flow.	for the OT environment and supports common OT protocols to provide protection of the OT network between logical and/or physical segments, as well as OT networks that face the IT or internet environment.	
B.20.4		The network architecture and devices have been reviewed regularly, at least annually, to ensure they are up-to-date, without obsolete rules and protocols.	#	#	#
B.20.5	Promoter	The organisation has defined and implemented a process to configure both wired and wireless networks securely, minimally using secure network authentication and encryption protocols and disabling Wi-Fi Protected Setup (WPS) to ensure that the network is secured and data is not lost or breached through the network.	For securing the organisation's connection to the cloud or communications between cloud environments, the organisation has implemented secure communication channels with up-to-date and approved protocols, e.g., use of encryption, cloud VPNs.	In situations where securing OT communications and networks is not appropriate or recommended, e.g., has a negative impact on OT operations or safety, the organisation has implemented compensating controls. Examples include: – where secure network authentication and encryption protocol cannot be implemented, using media access control (MAC) address filtering or other measures; and	#

				– where legacy OT devices only support insecure wireless connections, using physical controls such as limiting wireless network coverage range within a secured physical area.	
B.20.6		The organisation has defined and implemented a process to carry out network segmentation to segregate networks into private and public networks, with the private network holding business-critical data and having no connection to the internet to ensure that it is isolated from external threats.	#	The organisation has implemented segmentation (which can also include physical segmentation) to: – restrict and control communication and information flow between segments, based on the security requirements, risk and/or criticality; and – protect OT legacy systems that are insecure to provide isolation from threats propagating from other segments and/or the Internet.	As part of network segmentation, the organisation has implemented measures to manage the connectivity between its AI systems and other corporate systems, e.g., based on data sensitivity.
B.20.7	**Performer**	The organisation has established and implemented security policies and procedures outlining the requirements, guidelines and detailed steps to harden the network architecture, device and access security.	To harden its cloud environment, the organisation has incorporated cloud security best practices. Examples include: – using cloud network security groups for	#	#

			granular security policies at the resource level; – using container application-aware network monitoring tools for: ▪ automated determination of container networking surfaces, including both inbound ports and process-port bindings; ▪ detection of traffic flows between containers and other network entities; ▪ detection of network anomalies, e.g., unexpected traffic flows within the organisation's network, port scanning, or outbound access to potentially dangerous destinations; and ▪ detection of invalid or unexpected malicious processes and data introduced into the environment; and – using solutions such as cloud access security brokers (CASBs), or equivalent, leveraging frameworks such as secure access service edge (SASE) for network security in the cloud.		

B.20.8		The organisation has defined and assigned roles and responsibilities to oversee, manage and monitor network security to ensure that employees understand their assigned tasks.	#	#	#
B.20.9		The organisation has established and implemented network intrusion detection to monitor and detect malicious network traffic to ensure that it can be identified and addressed in a timely manner.	#	For network intrusion detection on OT networks, the organisation has established and implemented network intrusion detection solutions that are purpose-built or tailored for OT, i.e., network intrusion detection that has incorporated attack signatures for common various OT protocols, such as Modbus TCP, Distributed Network Protocol 3 (DNP3), and Inter-Control Center Communications Protocol (ICCP). When network intrusion detection solutions are not available for non-IP based protocols or controller-based operating systems in the OT environment, the organisation has considered compensating controls (e.g., anomaly detection systems).	#

B.20.10	**Advocate**	The organisation has established and implemented the policies and processes to evaluate the performance of network security devices in terms of their effectiveness in blocking malicious traffic and implementing improvements.	#	#	#
B.20.11		The organisation has established and implemented network intrusion prevention to block malicious network traffic and ensure that it is protected from threats.	#	For network intrusion prevention on OT networks, the organisation has established and implemented network intrusion prevention solutions that are purpose-built or tailored for OT: In situations where automated responses associated with network intrusion prevention systems may impact the OT environment, e.g., false positives, the organisation has implemented appropriate mitigation measures such as placing the network intrusion prevention systems at higher levels, e.g., the demilitarised zone (DMZ) interfaces in the OT network.	#

B.21 Domain: Incident response

This domain ensures that the organisation has formalised an incident response plan, with regular exercises conducted, to maintain the effectiveness of the current incident management set-up. This allows the organisation to detect, respond to and recover from cybersecurity incidents in a timely, professional and appropriate manner.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.21.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the mark of cyber hygiene under “A.9 Respond: Incident response” to ensure it is ready to detect, respond to and recover from cybersecurity incidents.	#	#	#
B.21.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the mark of cyber hygiene under “A.9 Respond: Incident response” to ensure it is ready to detect, respond to and recover from cyber incidents.	#	#	#
B.21.3	**Promoter**	The organisation has defined and applied measures to verify contact details and ensure that employees involved in the cybersecurity incident response plan are contactable to ensure a prompt response. Functional groups that are typically involved include: – senior management;	For cloud incident management, other functional groups, such as the cloud development team, may also be involved.	For OT incident management, other functional groups may also be involved: – IT personnel that are involved in OT operations; – OT personnel; and – security personnel and safety personnel.	For AI incident management, other functional groups, such as the AI development team, may also be involved.

		– incident response and/or cybersecurity team; – legal team; and – communications team.			
B.21.4		The organisation has defined and applied the process to perform cyber exercises to ensure that stakeholders are involved and know what to do when an incident occurs to ensure that they are well prepared.	The organisation has included cloud-specific scenarios in these cyber exercises.	The organisation has included OT-specific scenarios in these cyber exercises. In situations where there is heavy reliance or intersections between the OT customer and the OT supply chain, e.g. OT vendors, these exercises have included key external stakeholders in the OT supply chain.	The organisation has included AI-specific scenarios in these cyber exercises.
B.21.5	**Performer**	The organisation has defined and applied a process to carry out post-incident reviews of cyber exercises or cybersecurity incidents to identify areas for improvement and ensure that the incident response plan and process can be strengthened.	#	#	#
B.21.6		The organisation has defined and established policies and procedures outlining the requirements, guidelines and detailed steps to investigate incidents to gather evidence to ensure that the root cause can be identified.	Examples include: – using alerts from CSPM, SIEM, workload protection and network security monitoring; and – using cloud forensics to analyse the management plane, service and other	The organisation has integrated its OT-specific incident response with the organisational incident response plan. The policies and procedures established have included an evaluation of the response	The organisation has integrated its AI-specific incident response with the organisational incident response plan.

			logs and system forensics for containers and virtual machines.	actions required and their impact on OT operations, e.g., physical isolation of the compromised system may negatively impact OT operations and may result in disruption of operational performance or safety.	
B.21.7	**Advocate**	The organisation has established and incorporated cybersecurity-related incidents into its crisis management plan to respond to incidents of higher magnitude and impact to ensure that they are treated with the appropriate urgency.	#	#	#
B.21.8		The organisation has established and implemented a policy and process to report cybersecurity incidents and conclude the findings to the Board and/or senior management to ensure that they are kept informed.	#	#	#

B.22 Domain: Business continuity/Disaster recovery

This domain ensures that the organisation has identified critical assets and business processes so that recovery priorities can be established. Business continuity and disaster recovery management ensures that the organisation has developed and maintained capabilities, plans and testing to prepare employees, so that it is able to withstand disruptions and continue operations.

Clause	Preparedness tier	Classical cybersecurity	Cloud security	OT security	AI security
B.22.1	**Supporter**	Domain is not assessable for this tier. However, the organisation should consider using online resources to promote good cybersecurity practices internally. NOTE – In Singapore, CSA's cybersecurity toolkits for organisation leaders, employees and IT/cybersecurity personnel include content on cyber resilience	#	#	#
B.22.2	**Practitioner**	The organisation has identified the critical assets requiring high availability and implemented measures to ensure redundancies for them.	#	The organisation has identified critical connectivity and assets required for reduced or constrained operations in the event of a cybersecurity incident. For OT components that are not readily available, the organisation has taken steps to ensure redundancies/ replacements are available.	#
B.22.3	**Promoter**	The organisation has defined and implemented a business impact analysis to identify critical processes and expected recovery time objectives (RTOs) and recovery point objectives	#	#	#

		(RPOs) for business resumption.			
B.22.4		The organisation has defined and implemented a process to perform redundancy on systems to ensure the cyber resilience of its systems.	In the context of the cloud, this can include using cloud services that span multiple data centres and geographical regions for a single service to increase redundancy and resilience.	#	#
B.22.5	**Performer**	The organisation has established and implemented business continuity/disaster recovery policies outlining the requirements, roles and responsibilities and guidelines, including the RTO and RPO, to ensure that business resumption can be carried out according to the system's criticality.	#	When prioritising recovery activities, the organisation has factored in its risk assessment and developed an appropriate sequence for start-up activities of OT equipment that have operational dependencies.	#
B.22.6		The organisation has established and implemented a business continuity/disaster recovery plan to respond and recover from common business disruption scenarios, including those caused by cybersecurity incidents, to ensure cyber resilience.	The organisation has reviewed its CSPs' disaster recovery plan for restoring cloud services, including the recovery of the organisation's applications and data in the cloud, to ensure alignment with its own disaster recovery plan.	The organisation has determined the priority of recovery activities, e.g., recovering systems that support critical utilities before the OT systems. The organisation's business continuity/disaster recovery plan shall be documented in both electronic and paper form, and readily accessible.	#

B.22.7		The organisation performs regular reviews, at least annually, of the business continuity/disaster recovery plan to ensure it is kept up-to-date.	#	#	#
B.22.8		The organisation has established and implemented a policy and process to test its business continuity/disaster recovery plan regularly, at least annually, to ensure the effectiveness of the plan in achieving its objectives.	#	In situations where the testing the recovery plan is not feasible due to operational or safety considerations, the organisation has implemented alternative equivalents, such as laboratory testing or offline testing, to confirm the recovery procedures for OT equipment.	#
B.22.9	**Advocate**	The organisation monitors the RTO and RPO during business continuity/disaster recovery to ensure that they fall within targets and reports the findings to the Board and/or senior management.	#	#	#
B.22.10		The organisation performs coordinated business continuity/disaster recovery exercises with its third parties for an extended period to evaluate the effectiveness of the processes and procedures.	#	In situations where there is heavy reliance or intersections between the OT customer and the OT supply chain, e.g. OT vendors, these exercises have included key external stakeholders in the OT supply chain.	#