CSA CYBERSECURITY CERTIFICATION

Cyber Trust mark

Date of Publication: 01-08-2022 (First edition, revised)

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

Digitalisation creates new opportunities and COVID-19 has accelerated the rise of the digital economy. An increasingly digital way of life also increases organisational and individual exposure to cyber risks. Cybersecurity is a critical enabler of Singapore's digital economy. There is a need to build confidence in organisations to enable them to pursue the opportunities from digitalisation. Cybersecurity incidents often result in financial losses, tarnish business reputation and affect customers' trust, negating business investments and customers' confidence in the digital economy.

This document describes tiered cybersecurity standards that are designed to support the cybersecurity needs of a range of organisations. A framework has been developed to provide a guided approach to help organisations in their journey towards the implementation of cybersecurity in the organisation.

2 Scope

Organisations differ in terms of the nature of their business, size (which may be measured by parameters such as capital turnover or employment size) and the extent of digitalisation in their businesses. These have a corresponding impact on their cybersecurity risk profile. The CSA cybersecurity certification takes on a tiered approach to address different business profiles and needs as follows:

– The Cyber Essentials mark takes on a baseline control approach and is intended to protect organisations against the most common cyberattacks; and

– The Cyber Trust mark takes on a risk-based approach and is intended to enable organisations to put in place the relevant cybersecurity preparedness measures that commensurate with their cybersecurity risk profile.

Together, the Cyber Essentials mark and Cyber Trust mark provide a cybersecurity risk management framework for organisations. The Cyber Trust mark can be construed as a trust mark of distinction that recognizes the cybersecurity measures implemented in the organisation.

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 data that is vital to the operation of the organisation; where losing or exposing them can lead to detrimental impact, e.g., potential financial loses and legal issues.

3.2 Certification body

Certification body refers to an organisation that has been accredited for a sector to provide conformity assessment and to issue certificates of compliance which are recognised by the authorities.

3.3 Cloud shared responsibility model

The cloud shared responsibility model is a security framework used to segregate and ensure a common understanding of the security responsibilities shared between a cloud provider and its consumer.

3.4 Cyber hygiene

Cyber hygiene is a practice in cybersecurity to maintain and protect an organisation's systems from threat through adopting basic cyber health and security postures. It should be commensurate with the business activities of the organisation, with its associate risks.

3.5 Passphrase

Passphrase is typically a longer form of password that use a combination of random words, rather than just characters.

3.6 Trust mark

Trust mark is used to describe a visible label, or indicator, of the good practices that an organisation has put in place.

3.7 Use of "shall" and "should"

In this standard, the following verbal forms are used:

– "shall" indicates a requirement;

– "should" indicates a recommendation;

– "may" indicates a permission;

– "can" indicates a possibility or a capacity.

4 Cyber Trust mark

4.1 Concepts and principles

The Cyber Trust mark is targeted at larger or more digitalised organisations that have gone beyond cyber hygiene. These organisations may have higher risk levels and will correspondingly invest in expertise and resources to manage and protect their Information Technology (IT) infrastructure.

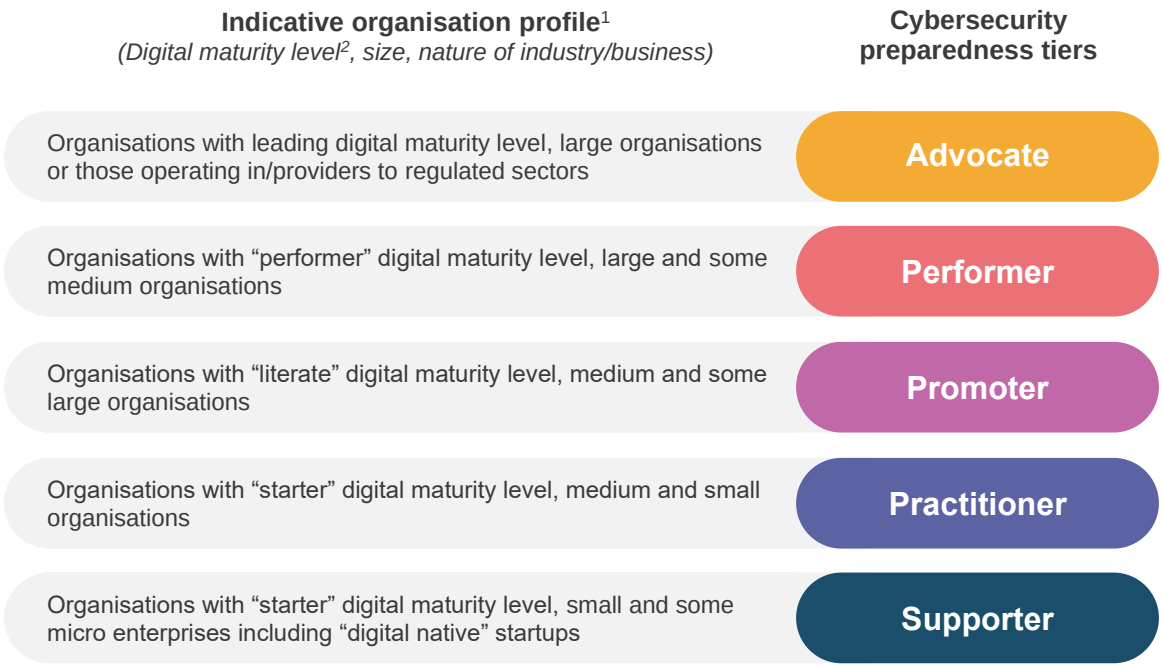
The key objective of the Cyber Trust mark is to serve as a mark of distinction to recognise organisations that are actively addressing cybersecurity risks and maintaining an adequate level of cybersecurity in their environment. The Cyber Trust mark also serves as a pathway for organisations to adopt international information security standards (e.g., ISO/IEC 27001:2013).

As the risk level of organisations vary, instead of prescribing specific cybersecurity measures, the Cyber Trust mark takes on a risk-based approach to guide organisations in identifying gaps in their

implementation of the cybersecurity preparedness measures so that their implementation commensurate with their cybersecurity risk profiles.

There are five (5) cybersecurity preparedness tiers in the Cyber Trust mark certification. Figure 1 shows the indicative target organisation profiles for each tier. Whilst indicative target organisation profiles for each tier are shown against dimensions such as the 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 have different risk profiles and correspondingly, need to be at different cybersecurity preparedness tiers as they may operate in different sectors, or their operations expose them to different nature of data and/or cybersecurity breach.



1 – Organisations of the same size may have different risk profiles, and correspondingly, need to be at different cybersecurity preparedness tiers
2 – 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 (22) cybersecurity preparedness domains, each focused around a specific cybersecurity theme. A series of cybersecurity preparedness statements are developed for each domain and organised into the five (5) cybersecurity preparedness tiers. These statements articulate the cybersecurity measures that organisations should consider and put in place, where relevant, to mitigate their inherent risk.

Organisations at a higher cybersecurity preparedness tier shall consider and correspondingly meet a higher number of domains. This is illustrated in Figure 2.

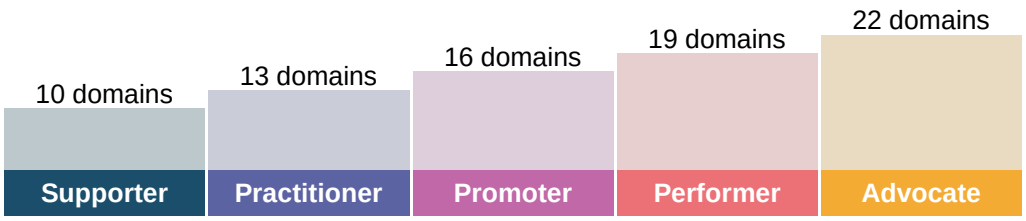


Figure 2 – Cyber Trust mark preparedness tiers and domains

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 Organisation profile

Organisations should establish if there is a match between their business needs and the protection and/or recognition accorded from being certified with the Cyber Trust mark.

The cybersecurity posture of an organisation depends on multiple factors and is different from organisation to organisation. The Cyber Trust mark does not prescribe that organisations need to be at a designated cybersecurity preparedness tier. Organisations should invest in the relevant and appropriate cybersecurity measures that commensurate with their risk profile.

4.3 Boundary of scope and statement of scope

Organisations should establish the boundary of scope for certification and determine the assessable components of the organisation's environment for the certification of Cyber Trust mark.

The scope of assessment and certification can cover the whole of the organisation's IT infrastructure, or a subset, e.g., a specific business unit, process or location. This is usually the sub-set that is critical or important for the organisation's core business. The organisation is also encouraged to include the whole IT infrastructure within the scope of assessment and certification, where feasible, so as to achieve the best protection.

The boundary of the scope shall be clearly defined, including the following:

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

The scope of assessment and certification shall be agreed between the organisation applying for certification and the certification body before assessment begins. The scope of assessment and certification shall be documented and the documentation shall include the following:

- The organisation chart depicting the business unit(s) within the scope;
- The context of the organisation's business;
- A system and network diagram;
- An inventory listing of devices and/or systems;
- An inventory listing of software and/or services;
- Locations from where the organisation operates or carries out the services that are to be covered as part of the certification; and
- The Cyber Trust mark self-assessment performed by the organisation[1].

The requirements for Cyber Trust mark shall apply to all devices[2], systems[3] and software that are within this boundary of scope.

The organisation applying for certification shall also define the statement of scope used to describe the scope of certification. In developing the statement of scope, the organisation may consider the following guiding principles:

a) Description of a critical or important aspect of the organisation's core business, e.g., "Provision of software development services in a software-as-a-service platform" in the context of a software development company;

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

c) If the organisation applying for certification conducts its business operations in multiple sites, the statement of scope can also make reference to the location of the site(s) included within the scope; and

d) The organisations may also consider taking on a phased approach, by starting with a smaller or narrow scope initially, and gradually expanding the scope of certification over time.

4.4 Pre-certification preparation by the organisation

Prior to engaging a certification body, the organisation shall complete the guided self-assessment template required for Cyber Trust mark certification.

This consists of a two-part assessment:

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

[1] See paragraph 4.4

[2] For organisations that implement Bring Your Own Device (BYOD), where employees use their own personal mobile devices for company tasks to access organisation's data or services, the scope of assessment and certification would include such devices.

[3] For organisations that adopt cloud-based software, the scope of assessment and certification would include such cloud-based services.

b) **Assessment of cybersecurity preparedness** – Concurrently in 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 in the organisation.

Referencing the assessment of the cybersecurity preparedness tier for each domain, the organisation then assesses its residual risk, which reflects the risk faced by the organisation when the mitigating cybersecurity measures are applied. The organisation shall also make a decision on the risk treatment of the residual risk(s) identified.

The outcome of the self-assessment will provide the organisation with an estimation of its cyber preparedness tier across the different domains, including a list of self-identified gaps against the applicable cyber 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.

Prior to engaging a certification body, the organisation may, optionally, engage a consultant to perform pre-certification audit on the scope it intends to submit for certification.

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

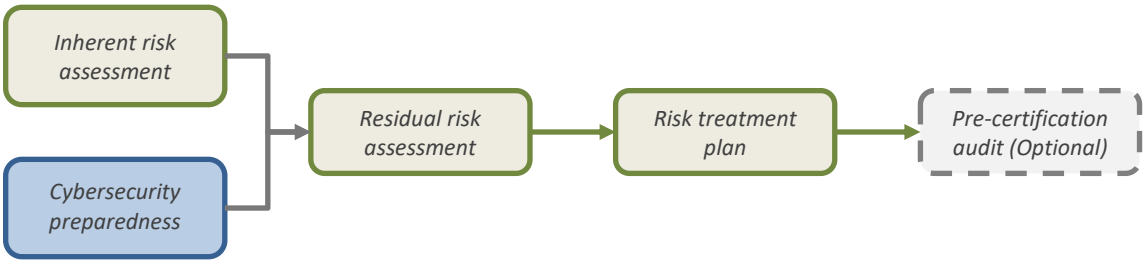


Figure 3 – Pre-certification preparation: Self-assessment and optional pre-certification audit

The Cyber Trust mark certification involves verification of implementation and effectiveness. For this reason, organisations applying for certification should ensure that they have approximately three (3) months of implementation data/logs in their systems by the time they are at the stage where assessors perform verification of implementation and effectiveness.

4.5 Risk scenarios in assessment of risk

The risk assessment template is pre-populated with risk scenarios that depict top/common cybersecurity incidents in organisations. Organisations assess their inherent risk by evaluating the likelihood and impact of these scenarios occurring in their environment. The categories of risk scenarios include:

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

b) **Human factor**
Cybersecurity incidents which happen due to human error or negligence.

c) **Infrastructure**
Cybersecurity incidents where the organisation's infrastructure is affected, causing disruption to the organisation's operations.

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

e) **Regulatory and compliance**
Non-compliance with regulatory standards which are 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.

4.6 Assessment of inherent and residual risk

4.6.1 Mapping risk scenarios to cybersecurity preparedness domains

The full list of risk scenarios is listed in Table 1**.** The relevant cybersecurity preparedness domains applicable to each risk scenario are also listed to provide further guidance to organisations.

Table 1 – Mapping risk scenarios to cybersecurity preparedness domains

Risk Ref	Risk Type	Risk Scenario	Applicable cybersecurity preparedness domains
1	Infrastructure	Attacker exploits a vulnerability in an obsolete operating system used by the organisation to host key application and gain unauthorised access into the application.	Domain: Risk management Domain: Audit Domain: Asset management Domain: System security Domain: Anti-virus/anti-malware
2	Infrastructure	Flooding of network with traffic causing disruption or inaccessibility of computer systems and network resources of the organisation.	Domain: Risk management Domain: System security Domain: Network security
3	Infrastructure	Attacker is able to gain access to the organisation's network and systems due to poor configuration of systems (e.g., have not changed from default configurations, etc.)	Domain: Backups Domain: System security Domain: Cyber threat management Domain: Network security

Risk Ref	Risk Type	Risk Scenario	Applicable cybersecurity preparedness domains
4	Infrastructure	Misconfiguration of the organisation's critical systems, causing disruption to the organisation's services and operations.	Domain: Audit Domain: Backups Domain: System security Domain: Business continuity/disaster recovery
5	Infrastructure	Attackers use malware to attack organisation's IT systems and penetrate the organisation's IT infrastructure, including servers, endpoints, and destroy sensitive and personal information.	Domain: Backups Domain: System security Domain: Anti-virus/anti-malware Domain: Cyber threat management Domain: Vulnerability assessment
6	Data Breach	Unauthorised users are able to access organisation's confidential and/or sensitive data from a stolen/loss corporate device, which leads to data leakage or disclosure of confidential and/or sensitive data.	Domain: Risk management Domain: Asset management Domain: Data protection and privacy Domain: Access control Domain: Network security
7	Data Breach	Attacker exploits a vulnerability in an organisation's application and gain access and able to extract confidential and/or sensitive data, including personal data.	Domain: Risk management Domain: System security Domain: Secure Software Development Life Cycle (SDLC) Domain: Access control Domain: Network security
8	Data Breach	Attacker takes advantage of compromised or otherwise unprepared devices to access organisation's confidential and/or sensitive data, which leads to data leakage or disclosure of confidential and/or sensitive data.	Domain: Risk management Domain: Data protection and privacy Domain: Domain: Bring Your Own Device (BYOD) Domain: System security Domain: Anti-virus/anti-malware Domain: Cyber threat management Domain: Network security
9	Data Breach	Use of portable storage devices (e.g., Universal Serial Bus (USB) drives, external hard disks) to transfer confidential and/or sensitive data can lead to data exfiltration by a malicious user.	Domain: Asset management Domain: Data protection and privacy
10	Data Breach	Unauthorised user is able to access data from IT assets that are not disposed properly leading to disclosure of confidential and/or sensitive data.	Domain: Asset management Domain: Data protection and privacy Domain: Audit

Risk Ref	Risk Type	Risk Scenario	Applicable cybersecurity preparedness domains
11	Human Factor	Disgruntled employee performing unauthorised modification to sensitive information to cause disruption to business operations.	Domain: Risk management Domain: Training and awareness Domain: Access control
12	Human Factor	Attacker sends phishing emails to employees containing malicious payload (e.g., attachments, Uniform Resource Locator (URL)), which can be used to further initiate cyberattacks into the organisation.	Domain: Risk management Domain: Training and awareness Domain: Access control Domain: Network security
13	Human Factor	Employee's negligence in handling confidential and/or sensitive data leading to disclosure of confidential and/or sensitive data.	Domain: Training and awareness Domain: Data protection and privacy
14	Human Factor	Inadequately skilled cyber resources within the organisation to manage cybersecurity incidents promptly, leading to a delayed response to a cybersecurity incident.	Domain: Governance Domain: Cyber strategy Domain: Incident response
15	Human Factor	High turnover rate of cybersecurity staff leading to a lack of resources to manage cybersecurity activities within the organisation.	Domain: Governance Domain: Cyber strategy
16	Physical Security	Unauthorised user is able to access data processing/sensitive information storage facility and damage or destroy the organisation's critical systems and data.	Domain: Risk management Domain: Backups Domain: Physical/environmental security Domain: Network security
17	Physical Security	Unauthorised user access to the organisation's network using wireless network access point and extracting personal and sensitive information.	Domain: Risk management Domain: BYOD Domain: Access control Domain: Network security Domain: Physical/Environmental security
18	Physical Security	Employees and visitors are not identifiable, resulting in missed detection of unauthorised access and malicious activities occurring.	Domain: Training and awareness Domain: Physical/environmental security
19	Physical Security	Environmental risk to the organisation's critical systems (e.g., fire, flood) which disrupts the operations of the systems.	Domain: Backups Domain: Business continuity/disaster recovery

Risk Ref	Risk Type	Risk Scenario	Applicable cybersecurity preparedness domains
20	Regulatory and Compliance	Organisation failing to comply with legal or regulatory requirements for data security. Non-compliance with the requirements results in financial penalties, operational disruption and reputational losses to the organisation.	Domain: Risk management Domain: Compliance Domain: Audit Domain: Data protection and privacy
21	Regulatory and Compliance	Organisation failing to comply with cybersecurity legal or regulatory requirements. Non-compliance with the requirements results in financial penalties, operational disruption and reputational losses to the organisation.	Domain: Risk management Domain: Compliance Domain: Audit
22	Regulatory and Compliance	Staff and vendors do not follow the organisation's security policies and processes, leading to non-compliance.	Domain: Policies and procedures Domain: Risk management Domain: Compliance Domain: Audit Domain: Training and awareness
23	Supply Chain	Vendor's negligence causing erroneous transactions in organisation's system.	Domain: Risk management Domain: Third-party risk and oversight
24	Supply Chain	Insecure vendor IT environment, allowing attackers to access organisation's network or data.	Domain: Risk management Domain: Access control Domain: Cyber threat management Domain: Third-party risk and oversight Domain: Network security
25	Supply Chain	Attackers cause disruption to third-party service providers, causing disruption to the organisation's services and operations.	Domain: Risk management Domain: Third-party risk and oversight Domain: Business continuity/disaster recovery

4.6.2 Assessing inherent risk – Risk likelihood and impact

Organisations assess their inherent risk by evaluating the likelihood and impact of the risk scenario occurring in their environment. 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 making an assessment of 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 potentially 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 making an assessment on 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 the business operations and/or quality of service.	Regulatory breach with material consequences which 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 the financial exposure.	Large impact on the customer experience and/or quality of service.	Regulatory breach with material consequences but which can 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 the financial exposure.	Moderate impact on the business operations and/or quality of service.	Regulatory breach with minimal consequences but which cannot be readily rectified.	Tarnish organisation's image with a specific group. Elements of public

Impact	Impact Score	Strategic	Financial	Operational	Regulatory Compliance (if applicable)	Brand value and Reputation
						expectations not met.
Minor	1	Minor impact on strategy, minimal reputational sensitivity.	Negligible impact on the 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.

4.6.3 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 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 taken 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 taken 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 time period specified by the organisation. The organisation may want to monitor the risks regularly to detect any changes if any.

Risk Measure	Risk Level	Risk Action	Description
1 – 4	Low	Monitor/Accept	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 the risk level.

4.6.4 Assessing residual risk

Organisations shall assess their residual risk after they have completed the assessment of their cybersecurity preparedness (this is covered in paragraph 4.7).

After this is completed, the organisation shall assess its residual risk, which reflects the risk faced by the organisation when the mitigating risk control measures are applied.

4.6.5 Risk heat map (for inherent and residual risk)

The resultant risk heat map that describes the inherent risk of the organisation is shown in Figure 4. A similar risk heat map is applicable for describing the residual risk of the organisation.

Impact

How severe is your organisation impacted if the risk scenario occurs?

Likelihood

What's the probability of the risk scenario occurring?

	Minor 1	Moderate 2	Significant 3	Serious 4	Major 5
Highly likely 5	Medium 5	Medium high 10	High 15	Critical 20	Critical 25
Likely 4	Low 4	Medium 8	Medium high 12	High 16	Critical 20
Possible 3	Low 3	Medium 6	Medium 9	Medium high 12	High 15
Unlikely 2	Low 2	Low 4	Medium 6	Medium 8	Medium high 10
Rare 1	Low 1	Low 2	Low 3	Low 4	Medium 5

Figure 4 – Risk heat map

4.6.6 Treatment of residual risk

After the organisation has completed the assessment of its inherent risk (described in paragraphs 4.6.2 and 4.6.3) the assessment of the cybersecurity preparedness tier for each domain (described in paragraph 4.7)), and the assessment of its residual risk (described in paragraph 4.6.4), 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 that 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 risk impact or both.
Avoid	Removing and eliminating the risk by removing the origin of the risk in its entirety. This treatment is not often applied unless terminating the activity which results in the risk arising does not materially affect an 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.

4.6.7 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

4.7 Assessment of cybersecurity preparedness

4.7.1 Cybersecurity preparedness tiers

The assessment of the cybersecurity preparedness of the organisation is intended to document the cybersecurity measures that organisations should consider and put in place, where relevant, to mitigate their risk.

As the risk level of organisations vary, instead of prescribing specific cybersecurity measures, the Cyber Trust mark takes a risk-based approach to guide organisations in identifying gaps in their implementation of the cybersecurity preparedness measures so that their implementation commensurate with their cybersecurity risk profile.

There are five (5) cybersecurity preparedness tiers in the Cyber Trust mark certification. Figure 1 shows the indicative target organisation profiles for each tier. The cybersecurity preparedness tier specific to the organisation's profile is determined through a guided risk assessment process in the Cyber Trust mark certification.

The Cyber Trust mark certification consists of twenty-two (22) cybersecurity preparedness domains. Each domain indicates a list of statements around a specific cybersecurity theme that organisations should consider and put in place, where relevant, to mitigate their inherent risk.

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 a higher cybersecurity preparedness tier shall meet a higher 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 *	●	●	●	●	●
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	16	19	22

* Measures in Cyber Essentials mark

The requirements and recommendations in Cyber Essentials mark are mapped to the “Supporter” and “Practitioner” tiers respectively in Cyber Trust.

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.

4.7.2 Assessment of implementation of cybersecurity preparedness domains

As indicated in paragraph 4.6.1, the risk assessment template is pre-populated with risk scenarios that depict top/common cybersecurity incidents in 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 fills in the risk assessment for each risk scenario, it shall refer to the corresponding cybersecurity preparedness domain(s) identified for that risk scenario, to document the extent of implementation in the organisation.

The description of the statements in each cybersecurity preparedness domain is organised in escalating order – the statements start 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 if the cybersecurity measure indicated is implemented within their 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 provides an indication of the cybersecurity preparedness tier of the organisation, and the organisation need not progress to the next cybersecurity preparedness tier statement for that domain (see Table 8).

For statements which 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 is not applicable to its environment. This shall be validated subsequently by their appointed certification body.

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

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

Preparedness tier	Description	Question	Organisation response *(Yes, No, Not applicable)*	Justification if "Not applicable"
Supporter	*Description*	*Question*		
Practitioner	*Description*	*Question*		
Promoter	*Description*	*Question*		
Performer	*Description*	*Question*		
Advocate	*Description*	*Question*		

4.7.3 Assessment of organisation cybersecurity 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 4.6.6, after the organisation has completed the assessment of its inherent risk (described in paragraphs 4.6.2 and 4.6.3) the assessment of the cybersecurity preparedness tier for each domain (described in paragraph 4.7), and the assessment of its residual risk (described in paragraph 4.6.4), 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.

4.8 Independent assessment by Certification Body

4.8.1 Approach and methodology for assessment

Following the completion of its self-assessment, the organisation shall approach any of the certification bodies appointed by CSA 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 business context of the organisation, critical services provided and information assets it holds to identify significant risk scenarios that the assessor should focus upon during the assessment.

Assessors shall employ a combination of assessment techniques including review and inspection of documents and other artefacts, conducting interviews, 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.

4.8.2 Staged assessment approach

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

a) **Verification of documentation (stage 1)** – This is 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)** – This is 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 a single 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 (6) 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 need to be re-conducted.

In stage 2 of the assessment, organisations shall ensure that they have approximately three (3) months of implementation data/logs in their systems so that assessors can perform verification of implementation and effectiveness.

4.8.3 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*: Total number of "Not applicable" responses to the cybersecurity preparedness statements shall be ≤ 20%

d) From tier 1 to tier *n*: 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 (2) stages of assessment.

4.8.4 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 (3) years.

The organisation shall undergo surveillance audit assessments against its Cyber Trust mark certification tier annually. This is to ensure the organisation's practices continually meet the applicable Cyber Trust mark cybersecurity preparedness statements for the applicable tier. After the 3-year validity of the Cyber Trust mark certification, the organisation may select to re-certify its Cyber Trust mark certification.

5 References

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

1. ISO/IEC 27001:2013 Information technology – Security techniques - Information security management systems — Requirements
2. ISO/IEC 27002:2013 Information technology – Security techniques - Code of practice for information security controls
3. Baseline Cyber Security Controls for Small and Medium Organisations V1.2 by Canadian Centre for Cyber Security
4. CIS Controls v8 by Centre for Internet Security
5. CIS Password Policy Guide by Centre for Internet Security
6. CISA Cyber Resilience Review (CRR) by US Department of Homeland Security (DHS) and CERT Division of CMU Software Engineering Institute
7. Cyber Essentials by UK National Cyber Security Centre (NCSC)
8. Cybersecurity Maturity Model Certification (CMMC) by US Department of Defence
9. Essential 8 by Australian Cyber Security Centre
10. Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool
11. Federal Risk and Authorisation Management Programme (FedRAMP) by US federal government
12. HiTrust by Health Information Trust Alliance
13. NIST Cybersecurity Frameworks
14. Payment Card Industry Data Security Standard (PCI DSS) by Visa, MasterCard, Discover Financial Services, JCB International and American Express.
15. SOC for Service Organisations by American Institute of Certified Public Accountants (AICPA)
16. Technology Risk Management Guidelines (TRMG) by Monetary Authority of Singapore (MAS)

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

B.1 Domain: Governance

The objective of this domain is to ensure that the organisation has practices in place to ensure that senior management is involved in the cybersecurity governance of the organisation. This includes overseeing the development and implementation of a cybersecurity strategy and roadmap to ensure that goals/objectives are defined and regularly tracked.

Clause	Preparedness tier	Description
B.1.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*
B.1.2	**Practitioner**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*
B.1.3	**Promoter**	The organisation has established and implemented practices to develop the importance of cybersecurity within its business context and communicate this to all relevant stakeholders such as employees, customers and partners.
B.1.4	**Performer**	The organisation has defined and allocated the roles and responsibilities to ensure that it is clear who is responsible to oversee the cybersecurity program implementation and manage cybersecurity risks within the organisation.
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.
B.1.6		The organisation has established cybersecurity goals/objectives which are reviewed and approved by the Board and/or senior management at least annually and implemented in the form of measures such as policies and procedures.

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.
B.1.8		The organisation has established and implemented practices to ensure that the Board and/or senior management are regularly updated on cybersecurity matters and key topics /decisions are discussed in a timely manner with regard to implementation of programs and initiatives based on the cybersecurity risks.

B.2 Domain: Policies and procedures

The objective of this domain is to ensure that cybersecurity policies and standards are established, implemented and communicated so that employees have clear direction and 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 protect the organisation from the evolving cyber threat landscape.

Clause	Preparedness tier	Description
B.2.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should consider the section 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 in CSA's cybersecurity toolkit for Small and Medium-sized Enterprise (SME) owners, organisation leaders and/or IT teams.*
B.2.2	**Practitioner**	*Domain is not assessable for this tier. However, the organisation should consider the section 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 in CSA's cybersecurity toolkit for SME owners, organisation leaders and/or IT teams.*
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.

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.
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 the 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 policy and process to ensure compliance with the cybersecurity policies and procedures.
B.2.9		The organisation has established and implemented policy and process to track and monitor non-compliance with policies, processes and procedures and ensure that the associated cybersecurity risks are addressed.

B.3 Domain: Risk management

The objective of this domain is to ensure that the organisation has established risk management practices in place to identify, assess, mitigate, monitor and report cybersecurity risks.

Clause	Preparedness tier	Description
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.
B.3.2		The organisation performs steps to analyse and prioritise the critical cybersecurity risks in the business environment to ensure that the more critical cybersecurity risks are addressed first.

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 clear on how to assess the cybersecurity risks.
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.
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 the 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 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.
B.3.10	**Advocate**	The organisation has established and implemented a cybersecurity risk management framework which 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.

B.4 Domain: Cyber strategy

The objective of this domain is to ensure that the organisation has established a cybersecurity strategy supported by a detailed roadmap and workplan so it can achieve planned targets and objectives over a time period and remain cyber resilient organisation-wide.

Clause	Preparedness tier	Description
B.4.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in CSA's cybersecurity toolkit for SME owners, organisation leaders and IT teams.*
B.4.2	**Practitioner**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in CSA's cybersecurity toolkit for SME owners, organisation leaders and IT teams.*
B.4.3	**Promoter**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in CSA's cybersecurity toolkit for SME owners, organisation leaders and IT teams.*
B.4.4	**Performer**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in CSA's cybersecurity toolkit for SME owners, organisation leaders and IT teams.*
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.
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 the 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, the roadmap and workplan at least annually to ensure alignment with business goals, taking into account the evolving cyber threat landscape.

B.5 Domain: Compliance

The objective of this domain is to ensure that 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	Description
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.
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 procedure 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 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 any non-compliance.

B.6 Domain: Audit

The objective of this domain is to ensure that the organisation has established an audit program to assess the effectiveness of policies, processes, procedures and controls against cybersecurity risks.

Clause	Preparedness tier	Description
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 in a timely manner.
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

The objective of this domain is to ensure that the organisation has instilled cybersecurity awareness and culture among its employees so that they do not form the weakest link in the organisation's defence.

Clause	Preparedness tier	Description
B.7.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark 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 Cyber Essentials mark 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 performs 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 performs measures to ensure that employees are assessed at the end of the awareness and training programmes and are required to pass the

		programmes to ensure 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.
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 skillset 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 to ensure that they can be bridged.
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

The objective of this domain is to ensure that hardware and software assets in the organisation environment are identified and tracked so that cybersecurity measures and/or processes can be implemented across the asset lifecycle. Active asset management allows for the organisation to

monitor for asset risks and enables control of assets within its environment so that only authorised assets are used and installed.

Clause	Preparedness tier	Description
B.8.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark 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 Cyber Essentials mark *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.
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.
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.
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 a policy 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.
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

The objective of this domain is to ensure that business-critical data in the organisation environment are identified and tracked so that cybersecurity measures and/or processes can be implemented across the asset lifecycle. It also ensures that data collection, processing, transfer and storage is secure to protect them from unauthorised access and/or disclosure.

Clause	Preparedness tier	Description
B.9.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark 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.9.2		The organisation has defined and applied a process to report any business-critical data (including personal data, company secrets, intellectual property, etc) breach and to ensure that stakeholders such as the management, relevant authorities and relevant individuals are kept informed.
B.9.3		The organisation that uses cloud service has established and implemented the cloud shared responsibility model with the Cloud Service Provider (CSP) in terms of data privacy and security (e.g., agreement with the CSP to establish clear roles and responsibilities between the organisation and the CSP).
B.9.4	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the Cyber Essentials mark 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.
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, etc) through information systems and programs in the organisation and implement relevant enforcement measures to ensure that they stay within the environment.
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).
B.9.8	**Performer**	The organisation has established and implemented data management policies and procedures through the guidelines, requirements and steps to handle business-critical data (including personal data, company secrets, intellectual property, etc.) at rest, in transit and in use securely.
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		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 not obsolete.
B.9.11	**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.
B.9.12		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, etc) in the organisation.
B.9.13		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

The objective of this domain is to ensure 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	Description
B.10.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark 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 Cyber Essentials mark 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.
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.
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 a consistent guidance and direction for performing backup and recovery in the organisation.
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 backup 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)

The objective of this domain is to ensure that the use of personal devices are 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	Description
B.11.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should consider the cybersecurity requirements in the Cyber Essentials mark 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 Cyber Essentials mark 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**	*Domain is not assessable for this tier. However, the organisation should consider the cybersecurity requirements in the Cyber Essentials mark 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.11.4	**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	**Advocate**	The organisation has established and implemented cybersecurity measures within BYOD to manage and enforce organisational security protections such as through the use of Mobile Device Management (MDM).
B.11.6		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.11.7		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.12 Domain: System security

The objective of this domain is to ensure 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	Description
B.12.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark under *A.6 Secure/Protect: Secure configuration* and *A.7 Update: Software updates* to ensure that the hardware and software uses secure and updated settings.
B.12.2	**Practitioner**	The organisation has implemented all the cybersecurity recommendations in the Cyber Essentials mark under *A.6 Secure/Protect: Secure configuration* and *A.7 Update: Software updates* to ensure that the hardware and software uses 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 in a timely manner.
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.
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.
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.
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.
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.
B.12.10		The organisation has established and implemented policies and procedures with the requirements, guidelines and detailed steps to perform and install patches/updates to ensure that the system(s) is/are patched or updated within the defined timeframes according to their priority.
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.
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, e.g., CIS configuration benchmarks.
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: Anti-virus/Anti-malware

The objective of this domain is to ensure that protection measures and technologies are implemented, maintained, and updated to continuously monitor and defend against malicious software which may disrupt or damage the network. This domain also addresses the processes put in place to manage successful malicious software attacks, so that further damage and spread to the network and environment is prevented.

Clause	Preparedness tier	Description
B.13.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark 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 Cyber Essentials mark 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 anti-virus and/or anti-malware solution(s) that is/are appropriate and recognised in the industry with features such as real-time malware detection and email protection, to ensure that it/they can protect the organisation adequately.
B.13.4		The organisation has established and implemented web filtering to protect the business from surfing malicious sites.
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.
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.
B.13.7	**Performer**	The organisation has defined and allocated the roles and responsibilities for employees to oversee, manage and maintain the anti-virus and/or anti-malware 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 with external parties and to share and verify information relating to cyberattacks which includes virus and/or malware attacks.
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 on indicators of compromise to ensure that anomalies and suspicious activities can be identified early.

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

The objective of this domain is to ensure 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	Description
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**	*Domain is not assessable for this tier.*
B.14.4	**Performer**	*Domain is not assessable for this tier.*
B.14.5	**Advocate**	The organisation has established and implemented a SDLC framework with cybersecurity measures and requirements to manage the software development life cycle to ensure that areas such as data integrity, authentication, authorisation, accountability and exception handling can be addressed.

B.14.6		The organisation has established and implemented security guidelines and requirements in its system and/or application development, e.g., secure coding to ensure that it adheres to the security principles.
B.14.7		The organisation has established and implemented the change management policy and process to ensure that changes or deployment to the production environment is reviewed and tested securely with a rollback plan in place to ensure that the change is controlled.
B.14.8		The organisation has established and implemented a policy and process to perform security testing on the system and/or application before deployment to ensure that the security weaknesses and vulnerabilities are identified.

B.15 Domain: Access control

The objective of this domain is to ensure 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 only granted on the principle of least privilege basis, and managed in a controlled and consistent manner.

Clause	Preparedness tier	Description
B.15.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark 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 Cyber Essentials mark 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 applied a process to approve and follow up on account access and role matrix review to ensure that unauthorised entry has been rectified and signed off.

B.15.5		The organisation has defined and applied a process to ensure that employees are assigned roles based on principle of least privilege and segregation of duties.
B.15.6		The organisation has established and implemented a secure logon policy and procedure on the requirements, guidelines and detailed steps of gaining access to sensitive and/or business-critical data as well as privileged access to ensure that the access is controlled and restricted.
B.15.7	**Performer**	The organisation has established and implemented a passphrase policy and procedure on the requirements, guidelines and detailed steps on setting and updating passphrases to provide guidance and direction on what constitutes strong passphrases.
B.15.8		The organisation has established and implemented a user access control policy and procedure on the requirements, guidelines and detailed steps to restrict and authorise users' access to the organisation's assets.
B.15.9		The organisation has established and implemented secure remote access policies and procedures on the requirements, guidelines and detailed steps to protect the information being accessed remotely.
B.15.10	**Advocate**	The organisation has established and implemented policies and processes to review any sign of access compromise and to report the result 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 and effective way of managing access.

B.16 Domain: Cyber threat management

The objective of this domain is to ensure 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	Description
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 on the requirements, guidelines and detailed steps to perform monitoring of security logs for threats and abnormality.
B.16.5		The organisation has defined and allocated the roles and responsibilities to carry out log monitoring and review on its systems, investigating the incidents and reporting to relevant stakeholders.
B.16.6		The organisation has implemented Security Information and Event Management (SIEM) to store the logs centrally for correlation and to ensure that the logs are monitored more effectively.
B.16.7		The organisation has established and implemented a security baseline profile on its systems to analyse and perform monitoring to ensure that anomalies are identified.
B.16.8		The organisation has established and implemented policies and procedures on the requirements, guidelines and detailed steps to carry out in response upon detection of abnormal or suspicious logs to ensure that they are investigated, reported and remediated in a timely manner.
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 against abnormal systems 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.

B.17 Domain: Third-party risk and oversight

The objective of this domain is to ensure 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 the services provided by any third-party service providers.

Clause	Preparedness tier	Description
B.17.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third parties have been implemented.* *They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*
B.17.2	**Practitioner**	*Domain is not assessable for this tier. However, the organisation should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third parties have been implemented.* *They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*
B.17.3	**Promoter**	*Domain is not assessable for this tier. However, the organisation should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third parties have been implemented.* *They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*

B.17.4	**Performer**	*Domain is not assessable for this tier. However, the organisation should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third parties have been implemented.* *They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*
B.17.5	**Advocate**	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.
B.17.6		The organisation has established and implemented measures to ensure that third parties are informed of their security obligations and to ensure that a security shared responsibility model is established for systems security and data protection; this shall include the organisation's CSPs and data centre service providers.
B.17.7		The organisation has established and implemented measures to assess their third parties before engaging them or on-boarding them to ensure that they meet all required security obligations based on the risks for the type of services provided by them.
B.17.8		The organisation has established and implemented measures to assess their third parties regularly based on security obligations agreed on systems security and data protection.
B.17.9		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

The objective of this domain is to ensure that vulnerability assessment and management are established to keep the organisation’s network and systems safe from known exploitation. This

domain also ensures processes to identify, evaluate, mitigate, and report on security vulnerabilities in systems and the software.

Clause	Preparedness tier	Description
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 assessment on its systems.
B.18.4		The organisation performs regular vulnerability assessment at least on an annual basis to perform non-intrusive scans on its systems to ensure that vulnerabilities are discovered.
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 on 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 in a timely manner.
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 being remediated according to their severity.
B.18.8	**Advocate**	The organisation has established and implemented a penetration test plan with the objectives, scope, rules of engagement to ensure that the penetration test can be performed safely.
B.18.9		The organisation performs a regular penetration test at least on an annual basis to discover and exploit security weakness(es) 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 in order 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

The objective of this domain is to ensure 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	Description
B.19.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should consider the section on cultivating cybersecurity leadership in the organisation, educating your employees on cybersecurity, securing your access and environment and protecting your information assets in CSA's cybersecurity toolkit for SME owners, organisation leaders and/or IT teams.*
B.19.2	**Practitioner**	The organisation has identified the physical/environmental risks in its environment and implemented detective measures to be alerted on threats to ensure that they are addressed in a timely manner.
B.19.3		The organisation has performed measures to protect its physical assets against internal and external threats, e.g., the use of cable locks to ensure that they are not stolen or tampered with.
B.19.4		The organisation has implemented physical security measures on its perimeters e.g., fence and gate to deter unauthorised access into the premises of the organisation.
B.19.5	**Promoter**	The organisation has defined and implemented the process to ensure that visitors are registered and authorised before having access to the premises of the organisation.
B.19.6		The organisation has defined and implemented the process to monitor its premises on a 24/7 basis, e.g., through the use of CCTV to deter and investigate on any physical/environmental threats.

B.19.7		The organisation has defined and applied the process to store and transport physical media containing business-critical data securely within and out of its premises to ensure that confidential and/or sensitive data are protected.
B.19.8	**Performer**	The organisation has established and implemented the policies and procedures on the requirements, guidelines and detailed steps for escalations and security access controls to minimise the impact and interference to its physical environment.
B.19.9		The organisation has defined and allocated the roles and responsibilities in detecting, mitigating and responding against physical/environmental risks to ensure that employees are clear of the tasks assigned to them.
B.19.10		The organisation has established and implemented the policies and procedures on the requirements, guidelines and detailed steps to perform reviews on the 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

The objective of this domain is to ensure that sufficient cybersecurity measures and/or processes are established to secure the confidentiality and accessibility of the organisation's network and data.

Clause	Preparedness tier	Description

B.20.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should ensure that A.2 Assets: Hardware and software domain, A.4.4 (f), (g), (h) and (k) under A.4 Secure/Protect: Virus and malware protection and A.6 Secure/Protect: Secure configuration in the Cyber Essentials mark on network security have been implemented.* *They should also consider the section on protecting your information assets in CSA's cybersecurity toolkit for SME owners and/or protecting your information assets and securing your access and environment in CSA's cybersecurity toolkit for organisation leaders and/or IT teams.*
B.20.2	**Practitioner**	The organisation has configured and implemented access control (e.g., whitelisting, blacklisting) to 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 basic packet filtering firewall to ensure that packets are filtered with more context for greater effectiveness.
B.20.4		The network architecture and devices have been reviewed regularly at least on an annual basis to ensure that they are up to date without obsolete rules and protocols.
B.20.5	**Promoter**	The organisation has defined and implemented the process to configure both wired and wireless networks securely**,** minimally with the use of secure network authentication and encryption protocol and disabling Wi-Fi Protected Setup (WPS) to ensure that the network is secured and data is not lost or breached through the network.
B.20.6		The organisation has defined and applied a process to carry out network segmentation to segregate into private and public networks with the private network holding all the business-critical data and having no connection to the Internet to ensure that it is isolated from external threats.
B.20.7	**Performer**	The organisation has established and implemented security policies and procedures with the requirements, guidelines and detailed steps to harden the network architecture, device and access security.

B.20.8		The organisation has defined and allocated roles and responsibilities to oversee, manage and monitor network security to ensure that the employees are clear of the tasks assigned to them.
B.20.9		The organisation has established and implemented network intrusion detection on the organisation's network to monitor and detect malicious network traffic to ensure that they can be identified and addressed in a timely manner.
B.20.10	**Advocate**	The organisation has established and implemented the policies and processes to evaluate the performance of the network security devices in terms of their effectiveness in blocking malicious traffic and carrying out improvements.
B.20.11		The organisation has established and implemented network intrusion prevention on the organisation's network to block malicious network traffic and ensure that it is protected from threats.

B.21 Domain: Incident response

The objective of this domain is to ensure 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 in an event of a cybersecurity incident.

Clause	Preparedness tier	Description
B.21.1	**Supporter**	The organisation has implemented all the cybersecurity requirements in the Cyber Essentials mark under *A.9 Respond: Incident response* to ensure that 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 Cyber Essentials mark under *A.9 Respond: Incident response* to ensure they are ready to detect, respond to, and recover from cyber incidents.
B.21.3	**Promoter**	The organisation has defined and applied measures to verify the contact details and ensure that the employees involved in the cybersecurity incident response plan are contactable to ensure that they are able to respond in a timely manner.

B.21.4		The organisation has defined and applied the process to perform cyber exercises to ensure that the stakeholders are involved and know what to do when an incident occurs to ensure that they are well prepared.
B.21.5	**Performer**	The organisation has defined and applied a process to carry out post-incident review against the cyber exercise or cybersecurity incident to identify areas of improvement and ensure that the incident response plan and process can be strengthened.
B.21.6		The organisation has defined and established the policies and procedures on the requirements, guidelines and detailed steps to conduct investigation into the incident to gather evidence to ensure that they are able to identify the root cause.
B.21.7	**Advocate**	The organisation has established and incorporated cybersecurity-related incidents into its crisis management plan to respond against 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 the 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

The objective of this domain is to ensure 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 the organisation is able to withstand disruptions and continue operations.

Clause	Preparedness tier	Description
B.22.1	**Supporter**	*Domain is not assessable for this tier. However, the organisation should consider the section on ensuring the business is cyber resilient in CSA's cybersecurity toolkit for SME owners, organisation leaders and/or IT teams.*
B.22.2	**Practitioner**	The organisation has identified the critical assets in the organisation that require high availability and performed measures to ensure that there are redundancies for them.
B.22.3	**Promoter**	The organisation has defined and applied the process of business impact analysis to identify the critical processes

		and expected Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for business resumption.
B.22.4		The organisation has defined and applied the process to perform redundancy on systems to ensure the cyber resilience of its systems.
B.22.5	**Performer**	The organisation has established and implemented the business continuity/disaster recovery policies with the requirements, roles and responsibilities and guidelines including the recovery time objectives (RTO) and recovery point objectives (RPO) to ensure that business resumption can be carried out in accordance with the system's criticality.
B.22.6		The organisation has established and implemented a business continuity/disaster recovery plan to respond and recover against the common business disruption scenarios including those caused by cybersecurity incidents to ensure cyber resiliency.
B.22.7		The organisation performs regular reviews at least on an annual basis on the business continuity/disaster recovery plan to ensure it is kept up to date.
B.22.8		The organisation has established and implemented the policy and process to test on its business continuity/disaster recovery plan regularly at least on an annual basis to ensure the effectiveness of the plan in achieving its objectives.
B.22.9	**Advocate**	The organisation performs monitoring on the RTO and RPO during business continuity/disaster recovery to ensure that they fall within the targets and report 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 of time to evaluate the effectiveness of the processes and procedures.