CSA CYBERSECURITY CERTIFICATION

Cyber Essentials mark

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

A publication by

CSA SINGAPORE

SG CYBER SAFE | CYBER ESSENTIALS

About the Cyber Security Agency of Singapore (CSA)

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

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

Contents

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 described 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 Essentials mark.

3 Terms and definitions

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

3.1 Business-critical data

Data within the organisation such as product, staff and financial 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 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 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 uses 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; and

– "can" indicates a possibility or a capacity.

4 Cyber Essentials mark

4.1 Concepts and principles

The Cyber Essentials mark is targeted at organisations with limited Information Technology (IT) and/or cybersecurity expertise and resources to dedicate towards protecting IT assets and personnel.

The key objective of the Cyber Essentials mark is to enable organisations with limited resources for cybersecurity to prioritise the cybersecurity measures needed, so that they can be protected against common cyberattacks. The Pareto principle, also known as the 80/20 rule, is a relevant guiding principle.

To simplify the implementation for organisations that are just starting out in their digitalisation and/or cybersecurity journey, the Cyber Essentials mark helps enterprises to prioritise the essential cybersecurity measures needed to protect the organisations against common, non-targeted attacks.

The Cyber Essentials mark also serves as a badge to recognise organisations that observe good cyber hygiene.

The security measures for the Cyber Essentials mark are organised in five (5) categories, listed in Table 1.

Table 1 – Security measures for Cyber Essentials mark

Category: Assets	
People	Equip employees with know-how to be the first line of defence
Hardware and software	Know what hardware and software the organisation has, and protect them
Data	Know what data the organisation has, where they are, and secure the data
Category: Secure/Protect	
Virus and malware protection	Protect from malicious software like viruses and malware
Access control	Control access to the organisation's data and services
Secure configuration	Use secure settings for the organisation's hardware and software
Category: Update	
Software updates	Update software on devices and systems
Category: Backup	
Back up essential data	Back up the organisation's essential data and store them offline[1]
Category: Respond	
Incident response	Be ready to detect, respond to, and recover from cybersecurity incidents

4.2 Organisation profile

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

The cybersecurity posture of an organisation depends on multiple factors and is different from organisation to organisation. The Cyber Essentials mark is targeted at resource-constrained organisations with limited IT and/or cybersecurity expertise and resources to dedicate towards protecting IT assets and personnel.

[1] Not connected to the operational network

Organisations with a higher risk profile and/or more resources for cybersecurity should invest in more comprehensive cybersecurity measures. Such organisations should also consider applying for the Cyber Trust[2] mark.

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 the Cyber Essentials 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 subset 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 scope shall be clearly defined, including as follows:

- 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 Essentials mark self-assessment performed by the organisation.

The requirements for Cyber Essentials mark shall apply to all devices[3], systems[4] 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:

[2] CSA Cybersecurity Certification: Cyber Trust mark

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

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

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.

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 Essentials mark certification.

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

4.5 Independent assessment by certification body

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 Essentials mark certification.

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

Assessors may perform inspection of documents and other artefacts to evaluate the relevant documentation and design of the cybersecurity measures implemented in the organisation.

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

4.6 Certification life cycle

Once the Cyber Essentials mark certification has been issued to an organisation, the certification shall remain valid for a period of two (2) years.

After the 2-year validity of the Cyber Essentials mark certification, the organisation may select to re-certify its Cyber Essentials mark certification. Alternatively, the organisation may also consider seeking Cyber Trust mark certification if its risk profile has changed.

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

5 References

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

1. 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

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

A.1.1 Introduction

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

A.1.2 Applicability

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

A.1.3 Objective

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

A.1.4 Provisions

The provisions for equipping the employees to be the first line of defence are as follows:

a) The organisation shall put in place cybersecurity awareness training for all employees to ensure that employees are aware of the security practices and behaviour expected of them. Organisations may meet this requirement in different ways, e.g., provide self-learning materials for employees or engaging external training providers.

b) Cyber hygiene practices and guidelines shall be developed for employees to adopt in their daily operations.

c) The cyber hygiene practices and guidelines should include topics to mitigate cybersecurity incidents arising from the human factor as follows:

- Protect yourself from phishing;
- Set strong passphrase and protect them;
- Protect your corporate and/or personal devices (used for work);
- Report cybersecurity incidents;
- Handle and disclose business-critical data carefully; and
- Work onsite and remotely in a secure manner.

d) Where feasible, the training content should be differentiated based on the role of the employees:

- Senior management or business leaders – e.g., developing a cybersecurity culture/mindset in the organisation or establishing a cybersecurity strategy or workplan.
- Employees – e.g., using strong passphrases and protecting the corporate and/or personal devices used for work.

e) As good practice, such cybersecurity awareness initiatives should be conducted at least annually to refresh employees' awareness.

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

A.2.1 Introduction

Knowledge about the environment is the foundation of an effective cybersecurity strategy. Taking stock of the hardware and software in the organisation is a foundational step to monitor and protect them; ensuring that the assets are (i) authorised to access the organisation's environment, and (ii) secured properly.

A.2.2 Applicability

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

Software within the scope of assessment and certification includes business applications, online accounts for which the business email address is used and other applications accessed either locally or remotely via the devices.

A.2.3 Objective

To actively manage the hardware and software assets in the organisation's environment. Having visibility of what assets belong to the organisation allows for steps to be taken to monitor and protect these assets. Active asset management also ensures that only authorised assets and devices are used and only authorised software are installed.

A.2.4 Provisions

The provisions for identifying and protecting what hardware and software the organisation has, and securing them, are as follows:

a) An up-to-date asset inventory of all the hardware and software assets shall be maintained in the organisation. Organisations may meet this requirement in different ways, e.g., use of spreadsheet or IT asset management software to maintain the IT asset inventory.

b) Hardware assets within the scope of certification may include servers, network devices, laptops and computers. If the scope of the certification includes hardware assets such as mobile devices and/or IoT devices:

Mobile devices	– Organisations should include company-issued mobile devices as part of its asset inventory, e.g., mobile phone and tablet.
IoT devices	– Organisations should include IoT devices used within the organisation as part of its asset inventory, e.g., Closed Circuit Television (CCTV), smart printer, smart television.

c) The inventory list should contain details of the hardware assets where available as follows:

- Hardware name/model;
- Asset tag[5]/serial number;
- Asset type;
- Asset location;
- Network address;
- Asset owner;
- Asset classification;
- Department;
- Approval/authorised date; and
- End of Support (EOS) date

d) Software assets within the scope of certification may include software applications used by the organisation. If the scope of certification includes a cloud environment:

Cloud	– Organisation shall include what is hosted on the cloud instances, e.g., software and Operating System (OS).

e) The inventory list should contain the details of the software assets where available, as follows:

- Software name;
- Software publisher;
- Software version;
- Business purpose;
- Asset classification;
- Approval/authorised date; and
- EOS date.

f) As good practice, the hardware and software asset inventory list should be reviewed at least bi-annually (twice per year).

g) Hardware and software assets that are unauthorised or have reached their respective EOS shall be replaced.

[5] The asset tag is intended to provide unique identification for each of the asset, e.g., it can be concatenated with acronyms of the asset type, department prefix and a running number to form a unique identifier.

h) In the event of any continued use of EOS assets, the organisation shall assess and understand the risk, obtain approval from senior management, and monitor it until the asset is replaced.

i) An authorisation process shall be developed to onboard new hardware and software into the organisation. Organisations may meet this requirement in different ways, e.g., email approval from senior management, ensuring that new hardware and software come from official or trusted sources, performing malware scans to verify that the asset is clean and maintaining asset whitelisting/blacklisting.

j) The date of authorisation of software and hardware shall be keyed into the asset inventory list after obtaining the relevant dispensation, e.g., obtaining email approval or through the use of an approval form.

k) Software and hardware without approval dates shall be removed.

l) Before disposing of any hardware asset, the organisation shall ensure that all confidential information have been deleted, e.g., encrypting hard disk before reformatting and overwriting it.

m) The organisation should carry out steps to ensure that the assets are disposed of securely and completely, e.g., destroy the hard disks physically or engage disk shredding services.

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

A.3.1 Introduction

Data is the organisation's most valuable business asset. Identifying the critical data in the organisation is the key foundational step to classify, monitor, and protect to ensure that only authorised employees can access it.

A.3.2 Applicability

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

A.3.3 Objective

To actively manage data in the organisation's environment. Having visibility of what type of data the organisation is collecting, processing and storing allows for steps to be taken to monitor and protect the data from unauthorised access and/or disclosure.

A.3.4 Provisions

The provisions for knowing what data the organisation has, where they are and securing them are as follows:

a) The organisation shall identify and maintain an inventory of business-critical data[6] in the organisation. Organisations may meet this requirement in different ways, e.g., using spreadsheet or asset inventory software. The inventory list shall contain details of the data as follows:

   – Description;
   – Data classification and/or sensitivity;
   – Location; and
   – Retention period.

b) Review of the inventory list should be carried out at least annually, or whenever there is any change to the data captured by the organisation.

c) The organisation shall establish a process to protect its business-critical data, e.g., password protected documents, encryption of personal data (at rest) and/or emails.

d) There shall also be measures in place to prevent the employees from leaking confidential and/or sensitive data outside of the organisation, e.g., disabling USB ports.

e) Before disposing of any paper-based (hard copy) media, the organisation shall carry out steps to ensure that those containing confidential and/or sensitive data have been securely shredded.

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

A.4.1 Introduction

Malicious software (or malware) is a key threat faced in the organisation when hardware and software are connected to the Internet. Malware is designed to attack the systems, devices and steal data. It can also enter through end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Malware can also evolve rapidly, which is why it is important to keep the detection of malware updated frequently to stay protected against the latest malware.

A.4.2 Applicability

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

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

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

A.4.3 Objective

To ensure that sufficient protection measures are in place to continuously monitor and defend against malicious software, as such malicious software can result in unauthorised access to the organisation's network and cause damage to the organisation's environment.

A.4.4 Provisions

The provisions for protecting the organisation from malicious software are as follows:

a) Anti-malware solutions shall be used and installed in endpoints to detect attacks on the organisation's environment. Examples of endpoints include laptop computers, desktop computers, servers and virtual environments.

b) Virus and malware scans shall be carried out to detect possible cyberattacks. Where feasible, scans should always be automated and remain active to provide constant protection.

c) Organisations shall enable auto-updates or configure the anti-malware solution to update signature files or equivalent (e.g., non-signature based machine learning solutions) to detect new malware. Where possible, these updates should take place at least daily to stay protected from the latest malware.

d) Anti-malware solution shall be configured to automatically scan the files upon access. This includes files and attachments downloaded from the Internet through the web browser or email and external sources such as from portable USB drives.

e) If the scope of certification includes mobile devices, IoT devices, cloud environment or use of web browser/email:

Mobile devices	– Anti-malware solution should be installed and running on mobile devices.
IoT devices	– Anti-malware solution should be integrated with the IoT devices, e.g., CCTV, smart television, smart printers, digital door lock.
Cloud	– Anti-malware solution should be deployed on the cloud platform.
Web browser/ email	– Only fully supported web browsers and email client software with security controls should be used. – Anti-phishing and spam filtering tools should be established for the web browser/email client software. – Web browsers and/or email plug-ins/extensions/add-ons that are not necessary should be disabled and/or removed. – Web filtering should be deployed to protect the business from malicious sites, where feasible.

f) Firewalls shall be deployed or switched on to protect the network, systems, and endpoints such as laptops, desktops, servers, and virtual environments. In an environment where there is an organisation's network setup, a network perimeter firewall shall be configured to analyse and accept only authorised network traffic into the organisation's network. Examples can include packet filter, Domain Name System (DNS) firewall and application-level gateway firewall with rules to restrict

and filter network traffic. Depending on the organisation's network setup, the firewall functionality may be integrated with other networking devices or be a standalone device.

g) In an environment where there are endpoints connecting to the Internet and/or cloud-based applications, a software firewall (host-based firewall) should be configured and switched on for all the endpoints in the organisation where available, e.g., turning on the built-in software firewall feature included in most operating systems or anti-malware solutions.

h) As good practice, firewall configurations and rules should ideally be reviewed and verified annually to protect the organisation's Internet-facing assets where applicable.

i) If the scope of certification includes mobile and/or IoT devices:

Mobile devices	– It is recommended that firewalls should be installed and enabled on employees' mobile devices.
IoT devices	– It is recommended that firewalls should be configured and enabled on IoT devices where possible.

j) The organisation shall ensure that its employees install/access only authorised software/attachments within the organisation from official or trusted sources.

k) The organisation shall ensure that employees are aware of the use of trusted network connections for accessing the organisation's data or business email, e.g., mobile hotspot, personal Wi-Fi, corporate Wi-Fi and Virtual Private Network (VPN).

l) The organisation shall ensure that its employees are aware of the need to report any suspicious email or attachment to the IT team and/or senior management immediately.

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

A.5.1 Introduction

Active user accounts and physical access are the source of entry to the hardware and software in the organisation's environment. Ensuring that only authorised users are given the access rights they need to perform their work helps to reduce the risk of information being stolen, or hardware and software being compromised.

A.5.2 Applicability

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

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

A.5.3 Objective

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

A.5.4 Provisions

The provisions for controlling who has access to the organisation's data and system are as follows:

a) Account management shall be established to maintain and manage the inventory of accounts. The organisation may meet this in different ways, e.g., using of spreadsheets or exporting the list from software directory services.

b) The account inventory list shall contain details for user, administrator, third-party, and service accounts not limited to the following:

   – Name;
   – Username;
   – Department;
   – Role/account type;
   – Date of access created; and
   – Last logon date.

c) The organisation shall have a process with the necessary approvals to grant and revoke access. The organisation may implement this in different ways, e.g., email approval or access request form. This shall be implemented when there are personnel changes such as onboarding of new staff or change of role(s) for employees. The following fields shall be captured as follows:

   – Name;
   – System to access;
   – Department;
   – Role/account type;
   – From date; and
   – To date.

d) Access shall be managed to ensure employees can access only the information and systems required for their job role.

e) Accounts with access rights that are no longer required or have exceeded the requested date shall have their access disabled or removed from the system. Shared, duplicate, obsolete and invalid accounts shall be removed.

f) The administrator account shall only be accessed to perform administrator functions with approval from the senior management.

g) Access shall be managed to ensure that third parties or contractors can access only the information and systems required for their job role. Such access shall be removed once they no longer require them.

h) Third parties or contractors working with sensitive information in the organisation shall sign a non-disclosure agreement form. The form should include disciplinary action(s) for failure to abide by the agreement.

i) Physical access control shall be enforced to allow only authorised employees/contractors to access the organisation's IT assets and/or environment, e.g., use of cable lock to lock the workstations and card access door lock to authenticate and authorise entry.

j) As good practice, account reviews should be carried out at least quarterly or whenever there are changes to the account list, e.g., during onboarding and offboarding processes or organisation restructuring.

k) Dormant or inactive accounts which have been inactive for a prolonged period, e.g., sixty (60) days should be removed or disabled.

l) The organisation shall change all default passwords and replace them with a strong passphrase, e.g., it should be at least twelve (12) characters long and include upper case, lower case, and/or special characters.

m) User accounts shall be disabled and/or locked out after multiple failed login attempts, e.g., after ten (10) failed login attempts, 'throttling' the rate of attempts[7].

n) The account password shall be changed in the event of any suspected compromise.

o) Where feasible, two-factor authentication (2FA) should be used for administrative access to important systems, such as an Internet- facing system containing sensitive or business-critical data. Organisations may implement this in different ways, e.g., use of an authenticator application on the mobile or one-time password (OTP) token.

p) Where feasible, trusted software to manage passphrases should be used to aide employee passphrase management.

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

A.6.1 Introduction

Hardware and software are usually shipped by the manufacturers with the default settings that are typically geared towards ease of deployment and ease of use. The lack of security considerations can be readily exploited if they are left unsecured in their default settings.

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

A.6.2 Applicability

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

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

A.6.3 Objective

To ensure that sufficient protection measures are in place to secure the configurations and settings of hardware and software so as to reduce the risk from attacks that take advantage of well-known default administrator passwords, exploits or vulnerabilities.

A.6.4 Provisions

The provisions for using secure settings for the organisation's hardware and software are as follows:

a) Security configurations shall be enforced for the assets including desktop computers, servers and routers. Organisations may meet this requirement in different ways, e.g., adopting industry recommendations and standards such as Center for Internet Security (CIS) benchmarks on configuration guidelines across multiple vendor products, running baseline security analyser and/or using system configuration scripts.

b) Weak or default configurations shall be avoided or updated before using them, e.g., changing default password and performing deep scanning with anti-malware solution instead of standard scan.

c) Insecure configurations and weak protocols shall be replaced or upgraded to address the associated vulnerabilities, e.g., using Hypertext Transfer Protocol Secure (HTTPS) over normal Hypertext Transfer Protocol (HTTP) to encrypt data communication and upgrading Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access 2/3 (WPA2/WPA3) to enhance the Wi-Fi security standards.

d) Features, services, or applications that are not in used shall be disabled or removed, e.g., disabling file sharing services, software macros and File Transfer Protocol (FTP) ports.

e) Automatic connection to open networks and auto-run feature of non-essential programs (other than backup or anti-malware solution, etc.) shall be disabled.

f) Logging should also be enabled for software and hardware assets where feasible, e.g., system, events and security logs.

g) As good practice, automatic lock/session log out should be enabled after fifteen (15) min of inactivity for the organisation's assets. These include user sessions on the laptop computer, server, non-mobile device, database, and administrator portal.

h) If the scope of certification includes mobile devices, IoT devices, and/or cloud environment:

Mobile devices – e.g., mobile phone, tablet	– Mobile devices should not be jail-broken or rooted. – Mobile device passcodes should be enabled. – Automatic mobile device locks should be activated after two (2) min of inactivity. – Mobile applications should only be downloaded from official or trusted sources.
IoT devices	– Network hosting the IoT devices should be separated from the network containing the organisation's assets and data. – Security features should be enabled on IoT devices, e.g., turning off device auto-discovery and Universal Plug and Play (UPnP). – In selecting IoT devices, the organisation should use devices rated by the Cybersecurity Labelling Scheme (CLS) (where available).
Cloud	– Security logging and monitoring should be turned on for cloud visibility, e.g., history of Application Programming Interface (API) calls, change tracking and compliance.

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

A.7.1 Introduction

Software vendors regularly provide software updates with new features and to address newly discovered security vulnerabilities. It is important to install these software updates as soon as they are released to prevent attackers from exploiting security vulnerabilities.

A.7.2 Applicability

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

A.7.3 Objective

To ensure regular application of updates to software and applications in a timely manner to ensure that devices and systems are constantly protected against security vulnerabilities.

A.7.4 Provisions

The provisions for updating software on devices and systems for security are as follows:

a) The organisation shall prioritise the implementation of critical or important updates for operating systems and applications (e.g., security patches) to be applied as soon as possible.

b) The organisation should carry out compatibility tests on updates for operating system and applications before installing them.

c) The organisation should consider enabling automatic updates for critical operating system and application patches where feasible so that they can receive the latest updates.

d) If the scope of certification includes mobile devices, IoT devices, and/or cloud environment:

Mobile devices – e.g., mobile phone, tablet	– The organisation should ensure that updates and patches for mobile devices are only downloaded from trusted sources (e.g., official app store from the manufacturer).
IoT devices	– The organisation should remove or replace any IoT devices (e.g., CCTV, printers) that are not receiving any software patches or updates.
Cloud	– The organisation should refer to the cloud shared responsibility model with its Cloud Service Provider (CSP). This will allow organisations to be aware of when the organisation is responsible for software updates and security patches, and when the CSP is responsible. – The organisation should have visibility on the software updates and security patches done by its CSPs. – The organisation should also have security requirements regarding software updates defined for its CSPs.

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

A.8.1 Introduction

Data backups are critical in enabling quick recovery from cybersecurity incidents such as ransomware or malware, but also physical incidents such as system failure, theft, or natural disasters.

A.8.2 Applicability

Essential business information within the scope of assessment and certification refers to information that is needed to restore services or operations of the organisation.

A.8.3 Objective

To ensure regular back up of all essential business information in a secure manner so that the organisation is able to restore and recover its business operations when cybersecurity incidents take place.

A.8.4 Provisions

The provisions for backing up essential data and storing them securely offline are as follows:

a) The organisation shall identify business-critical systems and those containing essential business information and perform backup. What needs to be backed up is guided by identifying what is needed for business recovery in the event of a cybersecurity incident. Examples of business-critical

systems include stock-trading system, railway operating and control system. Examples of essential business information include financial data and business transactions.

b) The backups shall be performed on a regular basis, with the backup frequency aligned to the business requirements and how many days' worth of data the organisation can afford to lose.

c) For non-business-critical systems or non-essential information, the backups should still be performed but at/on a lower frequency/long term basis.

d) The backup process should be automated where feasible.

e) If the scope of certification includes cloud environment:

Cloud	– The organisation shall understand the role and responsibility between itself and the CSP in terms of data backup, e.g., cloud shared responsibility model, scope, and coverage of the cloud service. – Data backup shall be carried out by the organisation, e.g., storing the backups in a hard disk drive, purchasing the backup services by the CSP, and adopting multiple clouds to be used as backups.

f) If the scope of certification includes hardware assets such as mobile devices and/or IoT devices:

Mobile devices	– Essential business information stored in mobile phones should be auto backed up and transferred to a secondary mobile phone or secondary storage for backup, e.g., SMS conversations or contact of an important client.
IoT devices	– IoT devices containing the organisation's essential information should be backed up manually where automatic backup is not available, e.g., sensors in farms to improve operational safety and efficiency and in healthcare to monitor patients with greater precision to provide timely treatment.

g) All backups shall be protected from unauthorised access and be restricted to authorised personnel only. Backups should minimally be password-protected.

h) Backups shall be stored separately (i.e., offline) from the operating environment. Where feasible, backups should be stored offsite, e.g., separate physical location.

i) Frequent backups such as daily or weekly backups should be stored online to facilitate quick recovery, e.g., cloud backup storage.

j) Longer term backups such as monthly backups shall be stored offline in an external secure storage location, e.g., password-protected USB flash drives, encrypted external hard disks and/or tape storage at an alternative office location.

k) As good practice, backups should be tested at least bi-annually, or more frequently, to ensure that business-critical systems and essential business information can be restored effectively.

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

A.9.1 Introduction

Cybersecurity incidents can have a huge impact on an organisation in terms of cost, productivity, and reputation. It is important to have a cybersecurity incident response plan to allow the organisation to respond quickly by streamlining decisions, outlining processes, and defining appropriate use of the technologies available during an event of a cybersecurity incident.

A.9.2 Applicability

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

A.9.3 Objective

To ensure the organisation has an incident response plan so that it can detect, respond to, and recover from cybersecurity incidents in a timely, professional, and appropriate manner.

A.9.4 Provisions

The provisions for being ready to detect, respond to, and recover from cybersecurity incidents are as follows:

a) The organisation shall establish an up-to-date basic incident response plan to guide the organisation on how to respond to common cybersecurity incidents. Examples include phishing, data breach, ransomware. The plan shall contain details as follows:

   – Clear roles and responsibilities of key personnel in the organisation involved in the incident response plan process.
   – Procedures to detect, respond, and recover from the common cybersecurity threat scenarios, e.g., phishing, ransomware, data breach.
   – Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management).

b) The incident response plan shall be made aware to all employees in the organisation that have access to the organisation's IT assets and/or environment.

c) The organisation should conduct post- incident review and incorporate learning points to strengthen and improve the incident response plan.

d) As good practice, the incident response plan should be reviewed at least annually.