TECHNICAL CODE

INFORMATION AND NETWORK SECURITY - MALAYSIA CRITICAL SECURITY CONTROLS (MYCSC)

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date: 23 May 2023

MCMC MTSFB TC G042:2023

Development of Technical Codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
https://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
https://www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Information and Network Security Sub Working Group under the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

Deloitte Business Advisory Sdn Bhd

Digital Nasional Berhad

Digi Telecommunication Sdn Bhd

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

Telekom Malaysia Berhad

U Mobile Sdn Bhd

Universiti Kuala Lumpur

Webe Digital Sdn Bhd

Foreword

This technical code for Information and Network Security - Malaysia Critical Security Controls (MYCSC) ('this Technical Code') was developed pursuant to the Section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Information and Network Security Sub Working Group under the Security, Trust and Privacy Working Group.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INFORMATION AND NETWORK SECURITY - MALAYSIA CRITICAL SECURITY CONTROLS (MYCSC)

1. Scope

This Technical Code provides a set of requirements and references which serves as a guidance for critical security controls adoption within the context of MCMC MTSFB TC G009.

This Technical Code provides guidelines covering the following:

a) Malaysia Critical Security Controls (MYCSC) framework and its relationships with the following:

   i) Centre for Internet Security Critical Security Controls version 8 (CIS CSC v8) asset type - Device, Application, Data, Network, and Users;

   ii) CIS CSC v8 security function - Identify, Protect, Detect, Respond and Recover (refer clause 5, 7 and Annex B); and

   iii) other relevant information security management standards.

b) MYCSC control requirement details and control objectives (refer clause 6 and Annex C); and

c) MYCSC mapping with other control requirements (refer clause 8 and Annex D):

   i) MCMC MTSFB TC G009;

   ii) ISO/IEC 27002:2022;

   iii) ITU-T X.1051;

   iv) CIS CSC v8; and

   v) National Institute of Standards and Technology (NIST).

The use of MYCSC and the associated critical security controls support and compliment the MCMC MTSFB TC G009. This Technical Code is not intended to replace other regulatory and industry frameworks, standards or guidelines.

The controls requirements set out are generic and intended to be applicable to all organisations, regardless of size, type or nature within the Communications and Multimedia Industry (CMI) in Malaysia. The applicability of this Technical Code covers on-premises, off-premises, cloud-based and hybrid operated by organisation itself and/or authorised third-party.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G009, *Information and Network Security - Requirements*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls*

Recommendation ITU-T X.1051, *Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

Centre of Internet Security, *CIS Critical Security Controls Version 8*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex A.

4. Terms and definitions

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

4.1 Administrator account

Dedicated accounts with escalated privileges and used for managing aspects of a computer, domain or the whole enterprise Information Technology (IT) infrastructure. Common administrator account subtypes include root accounts, local administrator and domain administrator accounts and network or security appliance administrator accounts.

4.2 Authorisation systems

A system or mechanism used to determine access levels and user or client privileges related to system resources including files, services, computer programs, data and application features. An authorisation system grants or denies access to a resource based on the user's identity. Examples of authorisation systems can include active directory, access control lists and role-based access control lists.

4.3 Critical security controls

Prioritised set of actions to be used as information security best practices that mitigate the most common attacks against systems and networks.

4.4 End-user devices

IT assets used among members of an enterprise during work, off-hours or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones and tablets, as well as desktops and workstations that are owned by the organisation and personally owned devices. Personally owned devices will be subjected to the organisation's full or partial policy and control. For the purpose of this Technical Code, end-user devices are a subset of enterprise assets.

4.5 Enterprise assets

Assets with the potential to store or process data. For the purpose of this Technical Code, enterprise assets include end-user devices, network devices, non-computing or Internet of Things (IoT) devices and servers, in virtual, cloud-based and physical environments.

4.6 Externally exposed

Refers to enterprise assets that are public facing and discoverable through domain name system reconnaissance and network scanning from the public internet outside of the enterprise's network.

4.7 Internal enterprise assets

Refers to non-public facing enterprise assets that can only be identified through network scans and reconnaissance from within an enterprise's network through authorised, authenticated or unauthenticated access. Internal enterprise assets may be operated by a third-party on behalf of the organisation located within or outside the organisation premises and connected securely to enterprise's network.

4.8 Mobile end-user devices

Small, enterprise issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this Technical Code, mobile end-user devices are a subset of end-user devices.

4.9 Network infrastructure

Refers to all the resources of a network that make network or internet connectivity, management, business operations and communication possible. It consists of hardware and software, systems and devices and it enables computing and communication between users, services, applications and processes. Network infrastructure can be cloud, physical or virtual.

4.10 Non-computing or Internet of Things (IoT) devices

Devices embedded with sensors, software and other technologies for the purpose of connecting, storing and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems and information technology sensors. For the purpose of this Technical Code, non-computing or IoT devices are a subset of enterprise assets.

4.11 Portable end-user devices

Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this Technical Code, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets.

4.12 Remote devices

Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing or IoT devices and servers.

4.13 Removable media

Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include Compact Discs (CDs), Digital Versatile Discs (DVDs) and Blu-ray discs, tape backups, as well as diskettes and Universal Serial Bus (USB) drives.

4.14 Service accounts

A dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created to own data and configuration files only. They are not intended to be used by user, except for performing administrative operations.

4.15 Social engineering

Refers to a broad range of malicious activities accomplished through human interactions on various platforms, such as email or phone. It relies on psychological manipulation to trick users into making security mistakes or giving away sensitive information.

4.16 Software assets

Also referred to as software in this Technical Code, these are the programs and other Operating Systems (OS) used within an enterprise asset. Software assets include among others OS, applications, covering both on-premises, off-premises, cloud-based and hybrid.

4.17 User account

An identity created for a person in a computer or computing system. For the purpose of this Technical Code, user accounts refer to standard or interactive user accounts with limited privileges and are used for general tasks such as reading email and surfing the web. User accounts with escalated privileges are covered under administrator accounts.

5. Malaysia Critical Security Controls (MYCSC) framework

5.1 Relationship with MCMC MTSFB TC G009, ITU-T X.1051 and CIS CSC v8 framework

MYCSC framework summarises the relationship between ITU-T X.1051 and CIS CSC v8 framework with the following MCMC MTSFB TC G009 control themes:

a) Organisation (Related to CIS CSC v8 type - Organisational and Basic).

b) Infrastructure (Related to CIS CSC v8 type - Foundational).

c) People (Related to CIS CSC v8 type - Organisational and Basic).

d) Environment (Related to CIS CSC v8 type - Basic).

5.2 Malaysia Critical Security Controls (MYCSC) framework

The design and development of MYCSC framework is based on the following 7 key principles:

a) Improve the clarity of the security requirements and controls and to be consistent with CIS CSC v8 and ISO/IEC 27002:2022.

b) Simplify the security controls for easy implementation and adoption of MYCSC framework.

c) Bring more focus on the latest security controls practises, security technology and emerging security problems.

d) Better align with other frameworks, such as the NIST Cybersecurity Framework (CSF), Payment Card Industry Data Security Standard (PCI DSS) and ISO/IEC 27002:2022.

e) Support the development of related products (e.g. measurements or metrics as in MCMC MTSFB TC G021, implementation guides).

f) Identification of Information and Network Security (INS) control themes, which defined in MCMC MTSFB TC G009, and there are Infrastructure, Organisation, Environment and People. The details of the controls as in Annex B.

The MYCSC framework consists of 26 controls which are adopted from CIS CSC v8 (18 controls) and ISO/IEC 27002:2022 (8 controls) security requirements as listed in Table 1.

Table 1. MYCSC framework

MYCSC controls	INS control theme			
	Organisation	Infrastructure	Environment	People
1. Inventory and control of enterprise assets		√		
2. Inventory and control of software assets		√		
3. Data protection		√		
4. Secure configuration of enterprise assets and software		√		
5. Account management		√		√
6. Access control management		√		
7. Continuous vulnerability management		√		
8. Audit log management		√		
9. Email and web browser protections	√	√		
10. Malware defences		√		
11. Data recovery		√		
12. Network infrastructure management		√		
13. Network monitoring and defence		√		
14. Security awareness and skills training				√
15. Service provider management				√
16. Application software security		√		
17. Incident response management	√			√
18. Penetration testing		√	√	√
19. Threat intelligence	√	√		
20. Information security for use of cloud services		√		
21. Physical security monitoring		√	√	
22. Information deletion			√	
23. Data masking			√	
24. Data leakage prevention			√	
25. Web filtering			√	
26. Secure coding				√

6. Malaysia Critical Security Controls (MYCSC)

MYCSC is not exhaustive and serves as a baseline to strengthen organisation's cyber security management practices.

Further details of the control requirements are also provided in Annex C together with the mapping against the CIS CSC v8.

6.1 Inventory and control of enterprise assets

Actively manage (inventory, track and correct) all enterprise assets (i.e. end-user devices, including portable and mobile, network devices, non-computing or IoT devices and servers) connected to the infrastructure physically, virtually, remotely and those within cloud environments, to accurately know the totality of assets that shall be monitored and protected within the enterprise. This will also support identifying unauthorised and unmanaged assets to remove or remediate.

6.1.1 Control justifications

Enterprises cannot defend what they do not know they have. Managing control of all enterprise assets plays a critical role in security monitoring, incident response, system backup and recovery. Enterprises shall know what data is critical to them and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

Unidentified assets can also have weak security configurations that can make them vulnerable to web-based or email-based malware and adversaries can leverage weak security configurations for traversing the network, once attackers are inside.

6.2 Inventory and control of software assets

Actively manage (inventory, track and correct) all software (i.e. OS and applications) on the network so that only authorised software is installed and executable, and any unauthorised and unmanaged software is found and prevented from being installed or executed.

6.2.1 Control justifications

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. Management of software assets is important to identify unnecessary security risks. An enterprise should review its software inventory to identify any enterprise assets running software that is not needed for business purposes.

For example, a new enterprise asset may be installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to make an inventory of the assets, understand, assess and manage all software connected to an enterprise’s infrastructure.

6.3 Data protection

Develop processes and technical controls to identify, classify, securely handle, retain and dispose data.

6.3.1 Control justifications

The enterprise’s loss of control over protected or sensitive data is a serious and often reportable business impact. While some data is compromised or lost because of theft or espionage, the vast majority are a result of poorly understood data management rules and user error. The adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise and even more important, it is a regulatory requirement for most controlled data.

It is important for an enterprise to develop a data management process that includes a data management framework, data classification guidelines and requirements for protection, handling, retention and disposal of data. There should also be a data breach process that plugs into the incident response plan and the compliance and communication plans.

To derive data sensitivity levels, enterprises need to catalogue their key types of data and the overall criticality (i.e. impact to its loss or corruption) to the enterprise. This analysis would be used to create an overall data classification scheme for the enterprise. Enterprises may use labels, not limited to 'Sensitive', 'Confidential 'and 'Public' and classify their data accordingly.

6.4 Secure configuration of enterprise assets and software

Establish and maintain the secure configuration of enterprise assets (i.e. end-user devices, including portable and mobile, network devices, non-computing or IoT devices and servers) and software (i.e. OS and applications). Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

6.4.1 Control justifications

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older and vulnerable protocols and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates shall manage and maintain over the life cycle of enterprise assets and software.

Configuration updates shall be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response and to support audits. This control is important to on-premises devices, as well as remote devices, network devices and cloud environments.

6.5 Account management

Use processes and tools to assign and manage authorisation to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software

6.5.1 Control justifications

It is easier for an external or internal threat actor to gain unauthorised access to enterprise assets or data through using valid user credentials than through hacking the environment. Administrative or highly privileged, accounts are a particular target, because they allow attackers to add other accounts or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise and sometimes not known about, only to be revealed in standard account management audits.

6.6 Access control management

Use processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator and service accounts for enterprise assets and software.

6.6.1 Control justifications

This control focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Accounts should only have the minimal authorisation needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralising this function is ideal.

6.7 Continuous vulnerability management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, to remediate and minimise, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

6.7.1 Control justifications

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders shall have timely threat information available to them about software updates, patches, security advisories, threat bulletins, etc. and they shall regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention and resources.

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. Defenders face challenges in scaling remediation across an entire enterprise and prioritising actions with conflicting priorities, while not impacting the enterprise's business or mission.

6.8 Audit log management

Collect, alert, review and retain audit logs of events that could help detect, understand or recover from an attack.

6.8.1 Control justifications

Log collection and analysis are critical for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyse them. Attackers use this knowledge to hide their location, malicious software and activities on victim machines. Due to poor or non-existent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records should show and not limited to, when and how the attack occurred, what information was accessed and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for a long period of time.

6.9 Email and web browser protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.

6.9.1 Control justifications

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data or an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering.

Additionally, as enterprises move to web-based email or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication and phishing reporting buttons.

6.10 Malware defence

Prevent or control the installation, spread and execution of malicious applications, code or scripts on enterprise assets.

6.10.1 Control justifications

Malicious software (sometimes categorised as viruses) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network and encrypting or destroying data. Malware is ever evolving and adaptive, as modern variants leverage machine learning techniques.

Malware defences shall be able to operate in this dynamic environment through automation, timely and rapid updating and integration with other processes like vulnerability management and incident response. They shall be deployed at all possible entry points and enterprise assets to detect, prevent spread or control the execution of malicious software or code.

6.11 Data recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

6.11.1 Control justifications

In the cybersecurity triad, Confidentiality, Integrity and Availability (CIA), the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs or other malicious actions that make a system insecure. These actions do not have to be malicious, human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

6.12 Network infrastructure management

Establish, implement and actively manage (i.e. track, report and correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

6.12.1 Control justifications

Secure network infrastructure is an essential defence against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often, introduced with default settings, monitoring for changes and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualised gateways, firewalls, wireless access points, routers and switches.

6.13 Security monitoring and defence

Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base. Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

6.13.1 Control justifications

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis and response.

It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies and support regulatory compliance for many enterprises.

6.14 Security awareness and skills training

Establish and maintain a security awareness program to influence behaviour among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

6.14.1 Control justifications

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware to get into an enterprise, than to find a network exploit to do it directly. Users themselves, both intentionally and unintentionally, can cause incidents because of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords or using the same password they use on public sites. The training shall be updated regularly. This will increase the culture of security and discourage risky workarounds.

6.15 Service provider management

Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

6.15.1 Control justifications

Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise. Reviewing the security of third parties has been a task performed for decades, there is not a universal standard for assessing security and many service providers are being audited by their customers multiple times a month, causing impacts to their own productivity. This is because every enterprise has a different checklist or set of standards to grade the service provider.

6.16 Application software security

Manage the security life cycle of in-house developed, hosted or acquired software to prevent, detect and remediate security weaknesses before they can impact the enterprise.

6.16.1 Control justifications

Applications provide a human-friendly interface to allow users to access and manage data in a way that is aligned to business functions. They also minimise the need for users to deal directly with complex and potentially error-prone system functions, like logging into a database to insert or modify files. Enterprises use applications to manage their most sensitive data and control access to system resources. Therefore, an attacker can use the application itself to compromise the data, instead of an elaborate network and system hacking sequence that attempts to bypass network security controls and sensors.

6.17 Incident response management

Establish a program to develop and maintain an incident response capability (e.g. policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.

6.17.1 Control justifications

The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened and what can be done to prevent it from happening again, defenders will just be in a perpetual whack-a-mole pattern.

After defining incident response procedures, the incident response team or a third-party, shall engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and potential impacts the enterprise faces. These scenarios help ensure that enterprise leadership and technical team members understand their role in the incident response process to help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes and unexpected dependencies, which can then be updated into the plan.

6.18 Penetration testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (i.e. people, processes and technology) and simulating the objectives and actions of an attacker.

6.18.1 Control justifications

Penetration tests are usually performed for specific purposes:

a) as a ‘dramatic’ demonstration of an attack, usually to convince decision-makers of their enterprise’s weaknesses;

b) as a means to test the correct operation of enterprise defences (‘verification’); and

c) to test that the enterprise has built the right defences in the first place (‘validation’).

6.19 Threat intelligence

Information relating to information security threats should be collected and analysed to produce threat intelligence.

6.19.1 Control justifications

Threat intelligence is about collecting and analysing information about existing or emerging threats to facilitate informed actions to prevent the threats from causing harm to the organisation or reduce the impact of such threats. This controls also is to provide awareness of the threat environment that can impact the organisation so that the organisation can take appropriate mitigation actions.

6.20 Information security for use of cloud services

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.

6.20.1 Control justifications

The organisation shall establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties. The organisation shall define and communicate how it intends to manage security risks associated with cloud services. It can be an extension or part of the existing approach for how an organisation manages services provided by external parties.

The use of cloud services involves shared responsibility for information security and collaborative effort between the Cloud Service Provider (CSP) and the organisation acting as the cloud service customer. It is essential that the responsibilities for both the CSP and the cloud service customer are defined and implemented appropriately.

6.21 Physical security monitoring

Premises should be continuously monitored for unauthorised physical access.

6.21.1 Control justifications

Physical premises shall be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical security information management software either managed internally or by a monitoring service provider. This control is to detect and deter unauthorised physical access.

6.22 Information deletion

Information stored in information systems and devices should be deleted when no longer required.

6.22.1 Control justifications

This control is to prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for data deletion.

6.23 Data masking

Data masking shall be used in accordance with the organisation's topic-specific policy on access control and business requirement, taking legal requirements into consideration.

6.23.1 Control justifications

This control is to limit the exposure of sensitive data including personally identifiable information and to comply with legal, statutory, regulatory and contractual requirements.

6.24 Data leakage prevention

Data leakage prevention measures shall be applied to systems, networks and endpoint devices that process, store or transmit sensitive information.

6.24.1 Control justifications

This control is to detect and prevent the unauthorised disclosure and extraction of information by individuals or systems.

Data leakage prevention shall be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (e.g. geopolitical, human, financial, commercial, scientific) which may be of interest for espionage or may be critical for the community. The data leakage prevention actions shall be oriented to confuse the adversary's decisions for example by replacing authentic information with false one, either as an independent action or as response to the adversary's intelligence actions.

6.25 Web filtering

Access to external websites shall be managed to reduce exposure to malicious content.

6.25.1 Control justifications

This control is to protect systems from being compromised by malware and to prevent access to unauthorised web resources.

The organisation shall reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material. A technique for achieving this works by blocking the Internet Protocol (IP) address or domain of the website(s) concerned. Some browsers and anti-malware technologies will do this automatically or can be configured to do so.

6.26 Secure coding

Secure coding principles shall be applied to software development.

6.26.1 Control justifications

This control is to ensure the software is written securely thereby reducing the number of potential information security vulnerabilities in the software. The organisation shall establish organisation-wide processes to provide good governance for secure coding. A minimum secure baseline shall be established and applied. Additionally, such processes and governance shall be extended to cover software components from third parties and open source.

7. Malaysia Critical Security Controls (MYCSC) mapping with CIS CSC v8 security function and INS control theme

MYCSC is to supplement the existing MCMC MTSFB TC G009 with the established global cyber defence framework by adapting the controls into the telecommunication environment information security management. MYCSC provides additional and specific requirements for the CMI. Details on MYCSC mapping as in Annex B.

8. Malaysia Critical Security Controls (MYCSC) mapping with other control requirements

MYCSC is designed to complement to an organisation existing or any information security management framework. MYCSC may be used as a reference to information security management framework such as NIST CSF v1.1, PCI DSS and ISO/IEC on Information Security Management System (ISMS).

MYCSC mapping with other major security controls standards requirements are provided in Annex D.

Annex A
(informative)

Abbreviations

AAA	Authentication, Authorisation and Auditing
AoC	Attestation of Compliance
API	Application Programming Interface
CDs	Compact Discs
CIA	Confidentiality, Integrity and Availability
CIS CSC v8	Centre for Internet Security Critical Security Controls version 8
CMI	Communication and Multimedia Industry
CSF	Cybersecurity Framework
CSP	Cloud Service Provider
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DVD	Digital Versatile Discs
EDR	Endpoint Detection and Response
GRC	Governance Risk and Compliance
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
INS	Information and Network Security
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Centre
ISMS	Information Security Management System
IT	Information Technology
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MYCSC	Malaysia Critical Security Controls
NaaS	Network-as-a-Service
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System

NIST	National Institute of Standards and Technology
OpenSSH	OpenBSD Secure Shell
OS	Operating System
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
SaaS	Software as a Service
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SOC 2	Service Organisation Control 2
SPF	Sender Policy Framework
SSH	Secure Shell
SSO	Single Sign-On
Telnet	Teletype Network
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2

Annex B
(normative)

Malaysia Critical Security Controls (MYCSC) mapping with CIS CSC v8 security function and MCMC MTSFB TC G009

Table B.1. MYCSC mapping with CIS CSC v8 security function and MCMC MTSFB TC G009

No	Control	Control details	CIS CSC v8 security function					Annex A of MCMC MTSFB TC G009			
			Identify	Protect	Detect	Respond	Recover	Organisation	Infrastructure	People	Environment
1	Inventory and control of enterprise assets	Refer 6.1	1.1 1.4	N/A	1.3 1.5	1.2	N/A	N/A	3.1 3.4 3.15	N/A	N/A
2	Inventory and control of software assets	Refer 6.2	2.1 2.2	2.5 2.6 2.7	N/A	2.3	N/A	N/A	3.1 3.4 3.15	N/A	N/A
3	Data protection	Refer 6.3	3.1 3.2 3.7- 3.9 3.10 - 3.13	3.7 3.8	3.14	N/A	N/A	N/A	3.7 3.9 3.16	N/A	N/A
4	Secure configuration of enterprise assets and software	Refer 6.4	4.1 - 4.9 4.11 4.12	N/A	N/A	4.10	N/A	N/A	3.4 3.15 3.18	N/A	N/A
5	Account management	Refer 6.5	5.1	5.2 5.4 5.6	N/A	5.3	N/A	N/A	3.4 - 3.7 3.10 3.13	N/A	5.1
6	Access control management	Refer 6.6	6.6	6.1 - 6.5 6.7 6.8	N/A	N/A	N/A	N/A	3.4 - 3.7 3.9	N/A	N/A
7	Continuous vulnerability management	Refer 6.7	7.5 7.6	7.1 7.3 7.4	N/A	7.2 7.7	N/A	N/A	3.12 3.18	N/A	N/A
8	Audit log management	Refer 6.8	N/A	8.1 8.3 8.4 8.10	8.2 8.5 8.6 - 8.9 8.11 8.12	N/A	N/A	N/A	3.10 3.13	N/A	N/A

Table B.1. MYCSC mapping with CIS CSC v8 security function and MCMC MTSFB TC G009
(continued)

No	Control	Control details	CIS CSC v8 security function					Annex A of MCMC MTSFB TC G009			
			Identify	Protect	Detect	Respond	Recover	Organisation	Infrastructure	People	Environment
9	Email and web browser protections	Refer 6.9	N/A	9.1 - 9.7	N/A	N/A	N/A	2.3	3.18	N/A	N/A
10	Malware defences	Refer 6.10	N/A	10.1 - 10.3 10.5 10.6	10.4 10.7	N/A	N/A	N/A	3.3 3.9 3.16	N/A	N/A
11	Data recovery	Refer 6.11	N/A	11.3	N/A	N/A	11.1 11.2 11.4 11.5	N/A	3.7 3.14	N/A	N/A
12	Network infrastructure management	Refer 6.12	12.4	12.1 - 12.3 12.5 - 12.8	N/A	N/A	N/A	N/A	3.12	N/A	N/A
13	Security monitoring and defence	Refer 6.13	N/A	13.4 13.5 13.7 - 13.10	13.1 - 13.3 13.6 13.11	N/A	N/A	N/A	3.4 3.15 3.17	N/A	N/A
14	Security awareness and skills training	Refer 6.14	N/A	14.1 - 14.9	N/A	N/A	N/A	N/A	N/A	4.1	N/A
15	Service provider management	Refer 6.15	15.1 - 15.3 15.5	15.4 15.7	15.6	N/A	N/A	N/A	N/A	4.2	N/A
16	Application software security	Refer 6.16	N/A	16.1 - 16.14	N/A	N/A	N/A	N/A	3.8 3.18	N/A	N/A
17	Incident response management	Refer 6.17	N/A	N/A	N/A	17.1 - 17.6	17.7 - 17.9	2.4 2.5	N/A	4.1	N/A
18	Penetration testing	Refer 6.18	18.1 18.2 18.5	18.3 18.4	N/A	N/A	N/A	N/A	3.12 3.13 3.18	/	/
19	Threat intelligence	Refer 6.19	N/A	N/A	N/A	N/A	N/A	/	/	N/A	N/A
20	Information security for use of cloud services	Refer 6.20	N/A	N/A	N/A	N/A	N/A	N/A	/	N/A	N/A
21	Physical security monitoring	Refer 6.21	N/A	N/A	N/A	N/A	N/A	N/A	/	N/A	/

Table B.1. MYCSC mapping with CIS CSC v8 security function and MCMC MTSFB TC G009
(continued)

No	Control	Control details	CIS CSC v8 security function					Annex A of MCMC MTSFB TC G009			
			Identify	Protect	Detect	Respond	Recover	Organisation	Infrastructure	People	Environment
22	Information deletion	Refer 6.22	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	/
23	Data masking	Refer 6.23	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	/
24	Data leakage prevention	Refer 6.24	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	/
25	Web filtering	Refer 6.25	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	/
26	Secure coding	Refer 6.26	N/A	N/A	N/A	N/A	N/A	N/A	N/A	/	N/A

Annex C
(normative)

Malaysia Critical Security Control (MYCSC) requirements

All identified parameters in Table C.1 to C.26 (e.g. frequency, length, duration) shall be defined based on organisation's policies and procedures. The control requirements are classified into 2 categories:

a) A control requirement that is defined as 'Shall' is considered as mandatory to be implemented by the CMI organisations.

b) A control requirement that is defined as 'Should' is considered as recommendation to be implemented by the CMI organisations.

Table C.1. Inventory and control of enterprise assets

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
1	1.1	Establish and maintain detailed enterprise asset inventory	a) Establish and maintain an accurate, detailed and up-to-date inventory of all enterprise assets with the potential to store or process data, to include end-user devices (including portable and mobile), network devices, non-computing or IoT devices and servers. b) Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset and whether the asset has been approved to connect to the network. c) For mobile end-user devices, MDM type tools can support this process, where appropriate. d) This inventory includes assets connected to the infrastructure physically, virtually, remotely and those within cloud environments. e) It includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. f) Review and update the inventory of all enterprise assets bi-annually or more frequently.	Shall	Devices	Identify
1	1.2	Address unauthorised assets	a) Ensure that a process exists to address unauthorised assets on a weekly basis. b) The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network or quarantine the asset.	Should	Devices	Respond

Table C.1. Inventory and control of enterprise assets *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
1	1.3	Utilise an active discovery tool	a) Utilise an active discovery tool to identify assets connected to the enterprise's network. b) Configure the active discovery tool to execute daily or more frequently.	Shall	Devices	Detect
1	1.4	Use DHCP logging to update enterprise asset inventory	a) Use DHCP logging on all DHCP servers or IP address management tools to update the enterprise's asset inventory. b) Review and use logs to update the enterprise's asset inventory weekly or more frequently.	Should	Devices	Identify
1	1.5	Use a passive asset discovery tool	a) Use a passive discovery tool to identify assets connected to the enterprise's network. b) Review and use scans to update the enterprise's asset inventory at least weekly or more frequently.	Should	Devices	Detect

NOTES:

1. DHCP is Dynamic Host Configuration Protocol.
2. IoT is Internet of Things.
3. IP is Internet Protocol.
4. MDM is Dynamic Host Configuration Protocol.

Table C.2. Inventory and control of software assets

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
2	2.1	Establish and maintain a software inventory	a) Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. b) The software inventory shall document the title, publisher, initial install or use date and business purpose for each entry, where appropriate, include the URL, app store(s), version(s), deployment mechanism and decommission date. c) Review and update the software inventory bi-annually or more frequently.	Shall	Applications	Identify
2	2.2	Ensure authorised software is currently supported	a) Ensure that only currently supported software is designated as authorised in the software inventory for enterprise assets. b) If software is unsupported, yet necessary for the fulfilment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. c) For any unsupported software without an exception documentation, designate as unauthorised. d) Review the software list to verify software support at least monthly or more frequently.	Shall	Applications	Identify
2	2.3	Address unauthorised software	a) Ensure that unauthorised software is either removed from use on enterprise assets or receives a documented exception. b) Review monthly or more frequently.	Shall	Applications	Respond
2	2.4	Utilise automated software inventory tools	Utilise software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Should	Applications	Detect
2	2.5	Allow list authorised software	a) Use technical controls, such as application allow listing, to ensure that only authorised software can execute or be accessed. b) Reassess bi-annually or more frequently.	Should	Applications	Protect

Table C.2. Inventory and control of software assets *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
2	2.6	Allow list authorised libraries	a) Use technical controls to ensure that only authorised software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. b) Block unauthorised libraries from loading into a system process. c) Reassess bi-annually or more frequently.	Shall	Applications	Protect
2	2.7	Allow list authorised scripts	a) Use technical controls, such as digital signatures and version control, to ensure that only authorised scripts, such as specific .ps1, .py, etc., files, are allowed to execute. b) Block unauthorised scripts from executing. c) Reassess bi-annually or more frequently.	Should	Applications	Protect

NOTE: URL is Uniform Resource Locator.

Table C.3. Data protection

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
3	3.1	Establish and maintain a data management process	a) Establish and maintain a data management process. b) In the process, address data sensitivity, data owner, handling of data, data retention limits and disposal requirements, based on sensitivity and retention standards for the enterprise. c) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Shall	Data	Identify
3	3.2	Establish and maintain a data inventory	a) Establish and maintain a data inventory, based on the enterprise's data management process. b) Inventory sensitive data, at a minimum. c) Review and update inventory annually, at a minimum, with a priority on sensitive data.	Should	Data	Identify
3	3.3	Configure data access control lists	a) Configure data access control lists based on a user's need to know. b) Apply data access control lists, also known as access permissions, to local and remote file systems, databases and applications.	Should	Data	Protect
3	3.4	Enforce data retention	a) Retain data according to the enterprise's data management process. b) Data retention shall include both minimum and maximum timelines.	Shall	Data	Protect
3	3.5	Securely dispose of data	a) Securely dispose of data as outlined in the enterprise's data management process. b) Ensure the disposal process and method are commensurate with the data sensitivity.	Shall	Data	Protect
3	3.6	Encrypt data on end-user devices	Encrypt data on end-user devices containing sensitive data (e.g., example implementations can include Windows BitLocker®, Apple FileVault®, Linux® dm-crypt).	Shall	Devices	Protect
3	3.7	Establish and maintain a data classification scheme	a) Establish and maintain an overall data classification scheme for the enterprise. b) Enterprises may use labels, such as 'Sensitive', 'Confidential' and 'Public' and classify their data according to those labels. c) Review and update the classification scheme annually or when significant enterprise changes occur that could impact this safeguard.	Should	Data	Identify
3	3.8	Document data flows	a) Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. b) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Should	Data	Identify

Table C.3. Data protection *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
3	3.9	Encrypt data on removable media	Encrypt data on removable media.	Should	Data	Protect
3	3.10	Encrypt sensitive data in transit	Encrypt sensitive data in transit (example implementations can include TLS and OpenSSH).	Should	Data	Protect
3	3.11	Encrypt sensitive data at rest	a) Encrypt sensitive data at rest on servers, applications and databases containing sensitive data. b) Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this safeguard. c) Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	Should	Data	Protect
3	3.12	Segment data processing and storage based on sensitivity	a) Segment data processing and storage based on the sensitivity of the data. b) Do not process sensitive data on enterprise assets intended for lower sensitivity data.	Should	Network	Protect
3	3.13	Deploy a DLP solution	Implement an automated tool, such as a host based DLP tool to identify all sensitive data stored, processed or transmitted through enterprise assets, including those located onsite or at a remote service provider and update the enterprise's sensitive data inventory.	Should	Data	Protect
3	3.14	Log sensitive data access	Log sensitive data access, including modification and disposal.	Should	Data	Detect

NOTES:

1. DLP is Data Loss Prevention.
2. OpenSSH is OpenBSD Secure Shell.
3. TLS is Transport Layer Security.

Table C.4. Secure configuration of enterprise assets and software

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
4	4.1	Establish and maintain a secure configuration process	a) Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing or IoT devices and servers) and software (OS and applications). b) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Shall	Applications	Protect
4	4.2	Establish and maintain a secure configuration process for network infrastructure	a) Establish and maintain a secure configuration process for network devices. b) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Shall	Network	Protect
4	4.3	Configure automatic session locking on enterprise assets	a) Configure automatic session locking on enterprise assets after a defined period of inactivity. b) For general purpose OS, the period shall not exceed 15 minutes. c) For mobile end-user devices, the period shall not exceed 2 minutes.	Shall	Users	Protect
4	4.4	Implement and manage a firewall on servers	a) Implement and manage a firewall on servers, where supported. b) Example implementations include a virtual firewall, OS firewall or a third-party firewall agent.	Shall	Devices	Protect
4	4.5	Implement and manage a firewall on end-user devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Should	Devices	Protect
4	4.6	Securely manage enterprise assets and software	a) Securely manage enterprise assets and software. b) Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as SSH and HTTPS. c) Do not use insecure management protocols, such as Telnet and HTTP, unless operationally essential.	Shall	Network	Protect
4	4.7	Manage default accounts on enterprise assets and software	a) Manage default accounts on enterprise assets and software, such as root, administrator and other pre-configured vendor accounts. b) Example implementations can include disabling default accounts or making them unusable.	Shall	Users	Protect

Table C.4. Secure configuration of enterprise assets and software *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
4	4.8	Uninstall or disable unnecessary services on enterprise assets and software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module or service function.	Should	Devices	Protect
4	4.9	Configure trusted DNS servers on enterprise assets	a) Configure trusted DNS servers on enterprise assets. b) Example implementations include configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	Should	Devices	Protect
4	4.10	Enforce automatic device lockout on portable end-user devices	a) Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. b) For laptops, do not allow more than 20 failed authentication attempts. c) For tablets and smartphones, no more than 10 failed authentication attempts. d) Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	Should	Devices	Respond
4	4.11	Enforce remote wipe capability on portable end-user devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices or when an individual no longer supports the enterprise.	Should	Devices	Protect
4	4.12	Separate enterprise workspaces on mobile end-user devices	a) Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. b) Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	Should	Devices	Protect

NOTES:

1. DNS is Domain Name System.
2. HTTP is Hypertext Transfer Protocol.
3. HTTPS is Hypertext Transfer Protocol Secure.
4. SSH is Secure Shell.
5. Telnet is Teletype Network.

Table C.5. Account management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
5	5.1	Establish and maintain an inventory of accounts	a) Establish and maintain an inventory of all accounts managed in the enterprise. b) The inventory shall include both user and administrator accounts. c) The inventory, at a minimum, should contain the person's name, username, start and stop dates and department. d) Validate that all active accounts are authorised, on a recurring schedule at a minimum quarterly or more frequently.	Shall	Users	Identify
5	5.2	Use unique passwords	a) Use unique passwords for all enterprise assets. b) Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	Shall	Users	Protect
5	5.3	Disable dormant accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Shall	Users	Respond
5	5.4	Restrict administrator privileges to dedicated administrator accounts	a) Restrict administrator privileges to dedicated administrator accounts on enterprise assets. b) Conduct general computing activities, such as internet browsing, email and productivity suite use, from the user's primary, non-privileged account.	Shall	Users	Protect
5	5.5	Establish and maintain an inventory of service accounts	a) Establish and maintain an inventory of service accounts. b) The inventory, at a minimum, shall contain department owner, review date and purpose. c) Perform service account reviews to validate that all active accounts are authorised, on a recurring schedule at a minimum quarterly or more frequently.	Should	Users	Identify
5	5.6	Centralise account management	Centralise account management through a directory or identity service.	Should	Users	Protect
NOTE: MFA is Multi-Factor Authentication.						

Table C.6. Access control management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
6	6.1	Establish an access granting process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Shall	Users	Protect
6	6.2	Establish an access revoking process	a) Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation or role change of a user. b) Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Shall	Users	Protect
6	6.3	Require MFA for externally exposed applications	a) Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. b) Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this safeguard.	Should	Users	Protect
6	6.4	Require MFA for remote network access	Require MFA for remote network access.	Should	Users	Protect
6	6.5	Require MFA for administrative access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Should	Users	Protect
6	6.6	Establish and maintain an inventory of authentication and authorisation systems	a) Establish and maintain an inventory of the enterprise's authentication and authorisation systems, including those hosted on-site or at a remote service provider. b) Review and update the inventory, at a minimum, annually or more frequently.	Should	Users	Identify
6	6.7	Centralise access control	Centralise access control for all enterprise assets through a directory service or SSO provider, where supported.	Should	Users	Protect

Table C.6. Access control management *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
6	6.8	Define and maintain role-based access control	a) Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. b) Perform access control reviews of enterprise assets to validate that all privileges are authorised, on a recurring schedule at a minimum annually or more frequently.	**Should**	Data	**Protect**

NOTES:

1. MFA is Multi-Factor Authentication.

2. SSO is Single Sign-On.

Table C.7. Continuous vulnerability management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
7	7.1	Establish and maintain a vulnerability management process	a) Establish and maintain a documented vulnerability management process for enterprise assets. b) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Shall	Applications	Protect
7	7.2	Establish and maintain a remediation process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly or more frequent, reviews.	Shall	Applications	Respond
7	7.3	Perform automated OS patch management	Perform OS updates on enterprise assets through automated patch management on a monthly or more frequent, basis.	Should	Applications	Protect
7	7.4	Perform automated application patch management	Perform application updates on enterprise assets through automated patch management on a monthly or more frequent, basis.	Should	Applications	Protect
7	7.5	Perform automated vulnerability scans of internal enterprise assets	a) Perform automated vulnerability scans of internal enterprise assets on a quarterly or more frequent, basis. b) Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	Should	Applications	Identify
7	7.6	Perform automated vulnerability scans of externally exposed enterprise assets	a) Perform automated vulnerability scans of externally exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. b) Perform scans on a monthly or more frequent, basis.	Should	Applications	Identify
7	7.7	Remediate detected vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly or more frequent, basis, based on the remediation process.	Should	Applications	Respond

NOTES:

1. OS is Operating System.

2. SCAP is Security Content Automation Protocol.

Table C.8. Audit log management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
8	8.1	Establish and maintain an audit log management process	a) Establish and maintain an audit log management process that defines the enterprise's logging requirements. b) At a minimum, address the collection, review and retention of audit logs for enterprise assets. c) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Shall	Network	Protect
8	8.2	Collect audit logs	a) Collect audit logs. b) Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Shall	Network	Detect
8	8.3	Ensure adequate audit log storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Shall	Network	Protect
8	8.4	Standardise time synchronisation	a) Standardise time synchronisation. b) Configure at least 2 synchronised time sources across enterprise assets, where supported.	Shall	Network	Protect
8	8.5	Collect detailed audit logs	a) Configure detailed audit logging for enterprise assets containing sensitive data. b) Include event source, date, username, timestamp, source addresses, destination addresses and other useful elements that could assist in a forensic investigation.	Should	Network	Detect
8	8.6	Collect DNS query audit logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.	Should	Network	Detect
8	8.7	Collect URL request audit logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.	Should	Network	Detect
8	8.8	Collect command-line audit logs	a) Collect command-line audit logs. b) Example implementations include collecting audit logs from PowerShell®, BASH™ and remote administrative terminals.	Should	Devices	Detect
8	8.9	Centralise audit logs	c) Centralise, to the extent possible, audit log collection and retention across enterprise assets.	Should	Network	Detect
8	8.10	Retain audit logs	d) Retain audit logs across enterprise assets for a minimum of 90 days.	Should	Network	Protect

Table C.8. Audit log management *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
8	8.11	Conduct audit log reviews	a) Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. b) Conduct reviews on a weekly or more frequent, basis.	**Should**	Network	**Detect**
8	8.12	Collect service provider logs	a) Collect service provider logs, where supported. b) Example implementations include collecting authentication and authorisation events, data creation and disposal events and user management events.	**Should**	Data	**Detect**

NOTES:

1. DNS is Domain Name System.

2. URL is Uniform Resource Locater.

Table C.9. Email and web browser protections

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
9	9.1	Ensure use of only fully supported browsers and email clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Shall	Applications	Protect
9	9.2	Use DNS filtering services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Shall	Network	Protect
9	9.3	Maintain and enforce network-based URL filters	a) Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. b) Example implementations include category-based filtering, reputation-based filtering or through the use of block lists. c) Enforce filters for all enterprise assets.	Should	Network	Protect
9	9.4	Restrict unnecessary or unauthorised browser and email client extensions	Restrict, either through uninstalling or disabling, any unauthorised or unnecessary browser or email client plugins, extensions and add-on applications.	Should	Applications	Protect
9	9.5	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the SPF and the DKIM standards.	Should	Network	Protect
9	9.6	Block unnecessary file types	Block unnecessary file types attempting to enter the enterprise's email gateway.	Should	Network	Protect
9	9.7	Deploy and maintain email server anti-malware protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	Should	Network	Protect

NOTES:

1. DKIM is Domain Keys Identified Mail.
2. DMARC is Domain-based Message Authentication, Reporting and Conformance.
3. DNS is Domain Name System.
4. SPF is Sender Policy Framework.
5. URL is Uniform Resource Locater.

Table C.10. Malware defences

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
10	10.1	Deploy and maintain anti-malware software	Deploy and maintain anti-malware software on all enterprise assets.	Shall	Devices	Protect
10	10.2	Configure automatic anti-malware signature updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	Shall	Devices	Protect
10	10.3	Disable autorun and autoplay for removable media	Disable autorun and autoplay auto-execute functionality for removable media.	Shall	Devices	Protect
10	10.4	Configure automatic anti-malware scanning of removable media	Configure anti-malware software to automatically scan removable media.	Shall	Devices	Detect
10	10.5	Enable anti-exploitation features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® DEP, WDEG or Apple® SIP and Gatekeeper™.	Should	Devices	Protect
10	10.6	Centrally manage anti-malware software	Centrally manage anti-malware software.	Should	Devices	Protect
10	10.7	Use behaviour-based anti-malware software	Use behaviour-based anti-malware software.	Should	Devices	Detect

NOTES:

1. DEP is Data Execution Prevention.
2. SIP is System Integrity Protection.
3. WDEG is Windows Defender Exploit Guard.

Table C.11. Data recovery

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
11	11.1	Establish and maintain a data recovery process	a) Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritisation and the security of backup data. b) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Shall	Data	Recover
11	11.2	Perform automated backups	a) Perform automated backups of in-scope enterprise assets. b) Run backups weekly or more frequently, based on the sensitivity of the data.	Shall	Data	Recover
11	11.3	Protect recovery data	a) Protect recovery data with equivalent controls to the original data. b) Reference encryption or data separation, based on requirements.	Shall	Data	Protect
11	11.4	Establish and maintain an isolated instance of recovery data	a) Establish and maintain an isolated instance of recovery data. b) Example implementations include, version controlling backup destinations through offline, cloud or off-site systems or services.	Shall	Data	Recover
11	11.5	Test data recovery	Test backup recovery quarterly or more frequently, for a sampling of in-scope enterprise assets.	Shall	Data	Recover

Table C.12. Network infrastructure management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
12	12.1	Ensure network infrastructure is up to date	a) Ensure network infrastructure is kept up to date. b) Example implementations include running the latest stable release of software and/or using currently supported NaaS offerings. c) Review software versions monthly or more frequently, to verify software support.	Shall	Network	Protect
12	12.2	Establish and maintain a secure network architecture	a) Establish and maintain a secure network architecture. b) A secure network architecture shall address segmentation, least privilege and availability, at a minimum.	Should	Network	Protect
12	12.3	Securely manage network infrastructure	a) Securely manage network infrastructure. b) Example implementations include version-controlled-infrastructure-as-code and the use of secure network protocols, such as SSH and HTTPS.	Should	Network	Protect
12	12.4	Establish and maintain architecture diagram(s)	a) Establish and maintain architecture diagram(s) and/or other network system documentation. b) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Should	Network	Identify
12	12.5	Centralise network AAA	Centralize network AAA.	Should	Network	Protect
12	12.6	Use of secure network management and communication protocols	Use secure network management and communication protocols (e.g., 802.1X, WPA2 enterprise or greater).	Should	Network	Protect
12	12.7	Ensure remote devices utilise a VPN and are connecting to an enterprise's AAA infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	Should	Devices	Protect

Table C.12. Network infrastructure management *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
12	12.8	Establish and maintain dedicated computing resources for all administrative work	a) Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. b) The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	**Should**	Devices	**Protect**

NOTES:

1. AAA is Authentication, Authorisation and Auditing.
2. HTTPS is Hypertext Transfer Protocol Secure.
3. NaaS is Network-as-a-Service.
4. SSH is Secure Shell.
5. VPN is Virtual Private Network.
6. WPA2 is Wi-Fi Protected Access 2.

Table C.13. Network monitoring and defence

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
13	13.1	Centralise security event alerting	a) Centralise security event alerting across enterprise assets for log correlation and analysis. b) Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. c) A log analytics platform configured with security-relevant correlation alerts also satisfies this safeguard.	Should	Network	Detect
13	13.2	Deploy a host-based intrusion detection solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	Should	Devices	Detect
13	13.3	Deploy a network intrusion detection solution	a) Deploy a network intrusion detection solution on enterprise assets, where appropriate. b) Example implementations include the use of a NIDS or equivalent CSP service.	Shall	Network	Detect
13	13.4	Perform traffic filtering between network segments	Perform traffic filtering between network segments, where appropriate.	Should	Network	Protect
13	13.5	Manage access control for remote assets	a) Manage access control for assets remotely connecting to enterprise resources. b) Determine amount of access to enterprise resources based on up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process and ensuring the operating system and applications are up to date.	Should	Devices	Protect
13	13.6	Collect network traffic flow logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	Should	Network	Detect
13	13.7	Deploy a host-based intrusion prevention solution	a) Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. b) Example implementations include use of an EDR client or host based IPS agent.	Should	Devices	Protect
13	13.8	Deploy a network intrusion prevention solution	a) Deploy a network intrusion prevention solution, where appropriate. b) Example implementations include the use of a NIPS or equivalent CSP service.	Should	Network	Protect

Table C.13. Network monitoring and defence *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
13	13.9	Deploy port-level access control	a) Deploy port-level access control. b) Port-level access control utilizes 802.1x or similar network access control protocols, such as certificates and may incorporate user and/or device authentication.	Should	Devices	Protect
13	13.10	Perform application layer filtering	a) Perform application layer filtering. b) Example implementations include a filtering proxy, application layer firewall or gateway.	Should	Network	Protect
13	13.11	Tune security event alerting thresholds	Tune security event alerting thresholds monthly or more frequently.	Should	Network	Detect

NOTES:

1. CSP is Cloud Service Provider.
2. EDR is Endpoint Detection and Response.
3. IPS is Intrusion Prevention System.
4. NIDS is Network Intrusion Detection System.
5. NIPS is Network Intrusion Prevention System.
6. SIEM is Security Information and Event Management.

Table C.14. Security awareness and skills training

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
14	14.1	Establish and maintain a security awareness program	a) Establish and maintain a security awareness program. b) The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. c) Conduct training at hire and, at a minimum, annually. d) Review and update content annually or when significant enterprise changes occur that could impact this safeguard.	Shall	N/A	Protect
14	14.2	Train workforce members to recognise social engineering attacks	Train workforce members to recognise social engineering attacks, such as phishing, pre-texting and tailgating.	Shall	N/A	Protect
14	14.3	Train workforce members on authentication best practices	a) Train workforce members on authentication best practices. b) Example topics include MFA, password composition and credential management.	Shall	N/A	Protect
14	14.4	Train workforce on data handling best practices	a) Train workforce members on how to identify and properly store, transfer, archive and destroy sensitive data. b) This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings and storing data and assets securely.	Shall	N/A	Protect
14	14.5	Train workforce members on causes of unintentional data exposure	a) Train workforce members to be aware of causes for unintentional data exposure. b) Example topics include mis-delivery of sensitive data, losing a portable end-user device or publishing data to unintended audiences.	Shall	N/A	Protect
14	14.6	Train workforce members on recognising and reporting security incidents	Train workforce members to be able to recognise a potential incident and be able to report such an incident.	Shall	N/A	Protect
14	14.7	Train workforce on how to identify and report if their enterprise assets are missing security updates	a) Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. b) Part of this training should include notifying IT personnel of any failures in automated processes and tools.	Shall	N/A	Protect

Table C.14. Security awareness and skills training *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
14	14.8	Train workforce on the dangers of connecting to and transmitting enterprise data over insecure networks	a) Train workforce members on the dangers of connecting to and transmitting data over, insecure networks for enterprise activities. b) If the enterprise has remote workers, training shall include guidance to ensure that all users securely configure their home network infrastructure.	**Shall**	N/A	**Protect**
14	14.9	Conduct role-specific security awareness and skills training	a) Conduct role-specific security awareness and skills training. b) Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers and advanced social engineering awareness training for high-profile roles.	N/A	N/A	**Protect**

NOTES:

1. IT is Information Technology.
2. MFA is Multi-Factor Authentication.
3. OWASP is Open Web Application Security Project.

Table C.15. Service provider management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
15	15.1	Establish and maintain an inventory of service providers	a) Establish and maintain an inventory of service providers. b) The inventory is to list all known service providers, include classification(s) and designate an enterprise contact for each service provider. c) Review and update the inventory annually or when significant enterprise changes occur that could impact this safeguard.	Shall	N/A	Identify
15	15.2	Establish and maintain a service provider management policy	a) Establish and maintain a service provider management policy. b) Ensure the policy addresses the classification, inventory, assessment, monitoring and decommissioning of service providers. c) Review and update the policy annually or when significant enterprise changes occur that could impact this safeguard.	Should	N/A	Identify
15	15.3	Classify service providers	a) Classify service providers. b) Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk and mitigated risk. c) Update and review classifications annually or when significant enterprise changes occur that could impact this safeguard.	Should	N/A	Identify
15	15.4	Ensure service provider contracts include security requirements	a) Ensure service provider contracts include security requirements. b) Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements and data disposal commitments. c) These security requirements shall be consistent with the enterprise's service provider management policy. d) Review service provider contracts annually to ensure contracts are not missing security requirements.	Shall	N/A	Protect

Table C.15. Service provider management *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
15	15.5	Assess service providers	a) Assess service providers consistent with the enterprise's service provider management policy. b) Assessment scope may vary based on classification(s) and may include review of standardised assessment reports, such as SOC 2 and PCI AoC, customised questionnaires or other appropriately rigorous processes. c) Reassess service providers annually, at a minimum or with new and renewed contracts.	Should	N/A	Identify
15	15.6	Monitor service providers	a) Monitor service providers consistent with the enterprise's service provider management policy. b) Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes and dark web monitoring.	Should	Data	Detect
15	15.7	Securely decommission service providers	a) Securely decommission service providers. b) Example considerations include user and service account deactivation, termination of data flows and secure disposal of enterprise data within service provider systems.	Should	Data	Protect

NOTES:

1. AoC is Attestation of Compliance.
2. PCI is Payment Card Industry.
3. SOC 2 is Service Organisation Control 2.

Table C.16. Application software security

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
16	16.1	Establish and maintain a secure application development process	a) Establish and maintain a secure application development process. b) In the process, address such items as secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code and application security testing procedures. c) Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.	Should	Applications	Protect
16	16.2	Establish and maintain a process to accept and address software vulnerabilities	a) Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. b) The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports and a process for intake, assignment, remediation and remediation testing. c) As part of the process, use a vulnerability tracking system that includes severity ratings and metrics for measuring timing for identification, analysis and remediation of vulnerabilities. Review and update documentation annually or when significant enterprise changes occur that could impact this safeguard. d) Third-party application developers need to consider this an externally facing policy that helps to set expectations for outside stakeholders.	Shall	Applications	Protect
16	16.3	Perform root cause analysis on security vulnerabilities	a) Perform root cause analysis on security vulnerabilities. b) When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code and allows development teams to move beyond just fixing individual vulnerabilities as they arise.	N/A	Applications	Protect
16	16.4	Establish and manage an inventory of third-party software components	a) Establish and manage an updated inventory of third-party components used in development, often referred to as a bill of materials, as well as components slated for future use. b) This inventory is to include any risks that each third-party component could pose. c) Evaluate the list at least monthly to identify any changes or updates to these components and validate that the component is still supported.	Should	Applications	Protect

Table C.16. Application software security *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
16	16.5	Use up-to-date and trusted third-party software components	a) Use up-to-date and trusted third-party software components. b) When possible, choose established and proven frameworks and libraries that provide adequate security. c) Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	Should	Applications	Protect
16	16.6	Establish and maintain a severity rating system and process for application vulnerabilities	a) Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritising the order in which discovered vulnerabilities are fixed. b) This process includes setting a minimum level of security acceptability for releasing code or applications. c) Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. d) Review and update the system and process annually.	Should	Applications	Protect
16	16.7	Use standard hardening configuration templates for application infrastructure	a) Use standard, industry-recommended hardening configuration templates for application infrastructure components. b) This includes underlying servers, databases and web servers and applies to cloud containers, PaaS components and SaaS components. c) Do not allow in-house developed software to weaken configuration hardening.	Should	Applications	Protect
16	16.8	Separate production and non-production systems	Maintain separate environments for production and non-production systems.	Should	Applications	Protect
16	16.9	Train developers in application security concepts and secure coding	a) Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. b) Training can include general security principles and application security standard practices. c) Conduct training at least annually and design in a way to promote security within the development team and build a culture of security among the developers.	Should	Applications	Protect

Table C.16. Application software security *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
16	16.10	Apply secure design principles in application architectures	a) Apply secure design principles in application architectures. b) Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of never trust user input. c) Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type and acceptable ranges or formats. d) Secure design also means minimising the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files and renaming or removing default accounts.	Should	Applications	Protect
16	16.11	Leverage vetted modules or services for application security components	a) Leverage vetted modules or services for application security components, such as identity management, encryption and auditing and logging. b) Using platform features in critical security functions will reduce developers' workload and minimise the likelihood of design or implementation errors. c) Modern OS provide effective mechanisms for identification, authentication and authorisation and make those mechanisms available to applications. d) Use only standardised, currently accepted and extensively reviewed encryption algorithms. e) OS also provide mechanisms to create and maintain secure audit logs.	Should	Applications	Protect
16	16.12	Implement code-level security checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	Should	Applications	Protect
16	16.13	Conduct application penetration testing	a) Conduct application penetration testing. b) For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. c) Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.	Should	Applications	Protect

Table C.16. Application software security *(concluded)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
16	16.14	Conduct threat modelling	a) Threat modelling is the process of identifying and addressing application security design flaws within a design before code is created. b) It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. c) The goal is to map out the application, architecture and infrastructure in a structured way to understand its weaknesses.	**Should**	Applications	**Protect**

NOTES:

1. OS is Operating System.
2. PaaS is Platform as a Service.
3. SaaS is Software as a Service.

Table C.17. Incident response management

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
17	17.1	Designate personnel to manage incident handling	a) Designate one key person and at least one backup, who will manage the enterprise's incident handling process. b) Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. c) If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. d) Review annually or when significant enterprise changes occur that could impact this safeguard.	Shall	N/A	Respond
17	17.2	Establish and maintain contact information for reporting security incidents	a) Establish and maintain contact information for parties that need to be informed of security incidents. b) Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, ISAC partners or other stakeholders. c) Verify contacts annually to ensure that information is up-to-date.	Shall	N/A	Respond
17	17.3	Establish and maintain an enterprise process for reporting incidents	a) Establish and maintain an enterprise process for the workforce to report security incidents. b) The process includes reporting timeframe, personnel to report to, mechanism for reporting and the minimum information to be reported. c) Ensure the process is publicly available to all the workforces. d) Review annually or when significant enterprise changes occur that could impact this safeguard.	Shall	N/A	Respond
17	17.4	Establish and maintain an incident response process	a) Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements and a communication plan. b) Review annually or when significant enterprise changes occur that could impact this safeguard.	Shall	N/A	Respond
17	17.5	Assign key roles and responsibilities	a) Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders and analysts, as applicable. b) Review annually or when significant enterprise changes occur that could impact this safeguard.	Should	N/A	Respond

Table C.17. Incident response management *(continued)*

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
17	17.6	Define mechanisms for communicating during incident response	a) Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. b) Mechanisms can include phone calls, emails or letters. c) Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. d) Review annually or when significant enterprise changes occur that could impact this safeguard.	Should	N/A	Respond
17	17.7	Conduct routine incident response exercises	a) Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. b) Exercises need to test communication channels, decision making and workflows. c) Conduct testing on an annual basis, at a minimum.	Should	N/A	Recover
17	17.8	Conduct post-incident reviews	a) Conduct post-incident reviews. b) Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	Shall	N/A	Recover
17	17.9	Establish and maintain security incident thresholds	a) Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. b) Examples can include abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. c) Review annually or when significant enterprise changes occur that could impact this safeguard.	Should	N/A	Recover

NOTES:

1. ISAC is Information Sharing and Analysis Centre.

2. IT is Information Technology.

Table C.18. Penetration testing

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
18	18.1	Establish and maintain a penetration testing program	a) Establish and maintain a penetration testing program appropriate to the size, complexity and maturity of the enterprise. b) Penetration testing program characteristics include scope (e.g., network, web application, API, hosted services and physical premise controls frequency), limitations (e.g., acceptable hours and excluded attack types), point of contact information, remediation (e.g., how findings will be routed internally) and retrospective requirements.	Should	N/A	Identify
18	18.2	Perform periodic external penetration tests	a) Perform periodic external penetration tests based on program requirements, no less than annually. b) External penetration testing shall include enterprise and environmental reconnaissance to detect exploitable information. c) Penetration testing requires specialised skills and experience and shall be conducted through a qualified party. d) The testing may be clear box or opaque box.	Should	Network	Identify
18	18.3	Remediate penetration test findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritisation.	Should	Network	Protect
18	18.4	Validate security measures	a) Validate security measures after each penetration test. b) If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	Should	Network	Protect
18	18.5	Perform periodic internal penetration tests	a) Perform periodic internal penetration tests based on program requirements, no less than annually. b) The testing may be clear box or opaque box.	Should	N/A	Identify
NOTE: API is Application Programming Interface.						

Table C.19. Threat intelligence

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
19	19.1	Threat intelligence	Refer 7.19.	Shall	N/A	N/A

Table C.20. - Information security for use of cloud services

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
20	20.1	Is for use of cloud services	Refer 7.20.	Shall	N/A	N/A

Table C.21. Physical security monitoring

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
21	21.1	Physical security monitoring	Refer 7.21.	Shall	N/A	N/A

Table C.22. Information deletion

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
22	22.1	Information deletion	Refer 7.22.	Shall	N/A	N/A

Table C.23. Data masking

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
23	23.1	Data masking	Refer 7.23.	Shall	N/A	N/A

Table C.24. Data leakage prevention

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
24	24.1	Data leakage prevention	Refer 7.24.	Shall	N/A	N/A

Table C.25. Web filtering

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
25	25.1	Web filtering	Refer 7.25.	Shall	N/A	N/A

Table C.26. Secure coding

Control	Sub-control	Title	Description	Control requirement	CSC v8 asset type	CSC v8 security function
26	26.1	Secure coding	Refer 7.26.	Shall	N/A	N/A

Annex D
(informative)

Malaysia Critical Security Controls (MYCSC) mapping with other control requirements

Table D.1. MYCSC mapping with NIST, PCI DSS and ISO/IEC

MYCSC sub-control (Refer Annex C)	NIST CSFv1.1	PCI DSS 3.2.1	ISO/IEC 27002:2022
MYCSC 1 - Inventory and control of enterprise assets			
1.1	ID.AM-1	2.4, 9.9.1, 11.1.1	5.9
1.2	N/A	N/A	
1.3	DE.CM-7	N/A	
1.4	DE.CM-7	N/A	
1.5	DE.CM-7	11.1, 11.1.2	
MYCSC 2 - Inventory and control of software assets			
2.1	ID.AM-2	2.4, 1.1.6	5.9
2.2	ID.AM-2	N/A	
2.3	DE.CM-7	N/A	
2.4	DE.CM-7	N/A	
2.5	DE.CM-7	N/A	
2.6	DE.CM-7	N/A	
2.7	PR.IP-1, PR.PT-3	N/A	
MYCSC 3 - Data protection			
3.1	PR.IP-6	N/A	5.12 5.13 5.14 8.24
3.2	ID.AM-5	9.6.1	
3.3	PR.AC-4	7.1, 7.11, 7.1.2 ,7.1.3	
3.4	N/A	N/A	
3.5	PR.DS-3, PR.IP-6	N/A	
3.6	N/A	N/A	
3.7	ID.AM-5	9.6.1	
	ID.RA-5	N/A	
3.8	DE.AE-1	1.1.3	
	ID.AM-3	N/A	
3.9	PR.PT-2	3.4	
3.10	PR.DS-2	2.1.1, 4.1, 4.1.1, 8.2.1	
3.11	PR.DS-1	3.4, 3.4.1, 8.2.1	
3.12	PR.AC-5	2.2.1, 2.4, 7.1	
3.13	PR.DS-5	N/A	

Table D.1. MYCSC mapping with NIST, PCI DSS and ISO/IEC *(continued)*

MYCSC sub-control (Refer Annex C)	NIST CSFv1.1	PCI DSS 3.2.1	ISO/IEC 27002:2022
3.14	N/A	11.5	5.12 5.13 5.14 8.24
MYCSC 4 - Secure configuration of enterprise assets and software			
4.1	PR.IP-1	2.2, 11.5	8.9
4.2	PR.IP-1	1.1.1, 1.1.2	
4.3	PR.IP-1	8.1.8	
4.4	N/A	1.1.4, 1.3.1	
4.5	N/A	1.4, 1.1.4	
4.6	N/A	N/A	
4.7	PR.AC-1	2.1, 2.1.1	
4.8	N/A	1.1.6, 1.2.1, 2.2.2, 2.2.5	
4.9	N/A	N/A	
4.10	N/A	N/A	
4.11	PR.AC-3	N/A	
4.12	N/A	N/A	
MYCSC 5 - Account management			
5.1	PR.AC-1	8.1, 8.1.1	5.16
5.2	N/A	N/A	
5.3	PR.AC-1	8.1.4	
5.4	PR.AC-4	7.1, 7.1.1, 7.1.2, 7.1.3	
5.5	PR.AC-1	N/A	
5.6	N/A	N/A	
MYCSC 6 - Access control management			
6.1	PR.AC-1	N/A	5.15
6.2	PR.AC-1	8.1.3	
	PR.IP-11	N/A	
6.3	PR.AC-7	8.3	
6.4	PR.AC-7	2.3, 8.3, 8.3.2	
	PR.AC-3	N/A	
6.5	PR.AC-7	8.3, 8.3.1, 8.3.2	
6.6	PR.AC-1, PR.AC-3	N/A	
6.7	PR.AC-1	N/A	
6.8	PR.AC-4	N/A	

Table D.1. MYCSC mapping with NIST, PCI DSS and ISO/IEC *(continued)*

MYCSC sub-control (Refer Annex C)	NIST CSFv1.1	PCI DSS 3.2.1	ISO/IEC 27002:2022
MYCSC 7 - Continuous vulnerability management			
7.1	ID.RA-1	N/A	8.8
7.2	ID.RA-1	11.2.1, 6.1	
7.3	N/A	6.2	
7.4	ID.RA-1	6.2	
7.5	DE.CM-8	11.2	
7.6	ID.RA-5	11.2	
	PR.IP-12	N/A	
7.7	N/A	N/A	
MYCSC 8 - Audit log management			
8.1	N/A	N/A	8.15
8.2	PR.PT-1	10.2, 10.3	
	DE.AE-3	N/A	
8.3	N/A	10.7	
8.4	PR.PT-1	10.4	
8.5	DE.AE-3	10.1	
	DE.CM-1	10.2.2, 10.2.4, 10.2.5, 10.3	
8.6	DE.AE-3	N/A	
8.7	DE.AE-3	N/A	
8.8	PR.PT-1, DE.AE-3	N/A	
8.9	N/A	10.5.3, 10.5.4	
8.10	N/A	10.7	
8.11	PR.PT-1	10.6, 10.6.1, 10.6.2	
	DE.AE-2, RS.AN-1	N/A	
8.12	DE.AE-3	N/A	
MYCSC 9 - Email and web browser protections			
9.1	PR.IP-1	N/A	8.7 8.23
9.2	PR.AC-5	N/A	
9.3	PR.AC-5	1.1.6, 11.4	
9.4	PR.IP-1	N/A	
9.5	N/A	N/A	
9.6	DE.CM-7, PR.AC-5	N/A	
9.7	DE.CM-4	N/A	

Table D.1. MYCSC mapping with NIST, PCI DSS and ISO/IEC *(continued)*

MYCSC sub-control (Refer Annex C)	NIST CSFv1.1	PCI DSS 3.2.1	ISO/IEC 27002:2022
MYCSC 10 - Malware defences			
10.1	DE.CM-4	5.1	8.7
10.2	DE.CM-4	5.1.1, 5.2, 11.4	
10.3	PR.PT-2	N/A	
10.4	DE.CM-4	N/A	
10.5	DE.CM-4	1.4	
10.6	DE.CM-4	11.4	
10.7	DE.CM-4	N/A	
MYCSC 11 - Data recovery			
11.1	PR.IP-9, ID.SC-5	N/A	5.30
11.2	PR.IP-4	12.10.1	
11.3	PR.IP-4	9.5, 9.5.1	
11.4	PR.PT-5	N/A	
11.5	PR.DS-6	N/A	
MYCSC 12 - Network infrastructure management			
12.1	N/A	N/A	8.20 8.21 8.22
12.2	PR.AC-5	1.1.6, 1.2.3, 2.2.2	
12.3	PR.AC-7, PR.DS-2	8.3	
12.4	ID.AM-4	N/A	
12.5	N/A	N/A	
12.6	PR.AC-7, PR.DS-2	2.1.1, 4.1.1	
12.7	PR.AC-3, PR.AC-7	N/A	
12.8	PR.AC-5	N/A	
MYCSC 13 - Network monitoring and defence			
13.1	N/A	10.5.2, 10.6.1	8.16 8.21
13.2	DE.CM-1	11.4	
13.3	DE.CM-1	11.4	
13.4	PR.AC-5	N/A	
13.5	PR.AC-3, PR.AC-7, PR.MA-2, DE.CM-7	N/A	
13.6	DE.CM-1	N/A	
13.7	DE.CM-1	11.4	
13.8	DE.CM-1	11.1, 11.4	
13.9	PR.AC-1	1.1.6, 1.2	
13.10	PR.PT-3	1.1.4, 1.2, 1.3.2 -1.3.5, 6.6	
13.11	DE.AE-5	N/A	

Table D.1. MYCSC mapping with NIST, PCI DSS and ISO/IEC *(continued)*

MYCSC sub-control (Refer Annex C)	NIST CSFv1.1	PCI DSS 3.2.1	ISO/IEC 27002:2022
MYCSC 14 - Security awareness and skills training			
14.1	ID.AM-6, ID.GV-1, PR.AT-1	9.9.3, 12.6, 12.6.1, 12.6.2	6.3
14.2	PR.AT-1	N/A	
14.3	PR.AT-1	N/A	
14.4	PR.AT-1	12.6	
14.5	PR.AT-1	N/A	
14.6	PR.AT-1	N/A	
14.7	PR.AT-1	N/A	
14.8	PR.AT-1	N/A	
14.9	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5	12.10.4, 6.5	
MYCSC 15 - Service provider management			
15.1	ID.SC-2	N/A	5.19 5.20 5.21 5.22
15.2	ID.GV-2, ID.SC-1	N/A	
15.3	ID.SC-2	N/A	
15.4	ID.SC-3, PR.AT-3	N/A	
15.5	ID.SC-4, ID.SC-2	N/A	
15.6	DE.CM-6	N/A	
15.7	PR.AC-1	N/A	
MYCSC 16 - Application software security			
16.1	PR.IP-1	6.3, 6.5	8.25 8.26 8.28
16.2	RS.AN-5	6.3.2	
16.3	RS.AN-1	N/A	
16.4	ID.AM-2	N/A	
16.5	PR.IP-2	6.2	
16.6	RS.AN-1	6.1	
16.7	PR.IP-1	2.2	
16.8	PR.DS-7	6.4.1, 6.4.2	
16.9	PR.AT-1, PR.AT-2	6.5, 6.5.1 - 6.5.10	
16.10	PR.IP-2	N/A	
16.11	PR.DS-1, PR.DS-2	N/A	
16.12	PR.IP-2	6.3.2	
16.13	N/A	N/A	
16.14	PR.AC-5, PR.DS-5, PR.DS-8, PR.IP-7	N/A	

Table D.1. MYCSC mapping with NIST, PCI DSS and ISO/IEC *(concluded)*

MYCSC sub-control (Refer Annex C)	NIST CSFv1.1	PCI DSS 3.2.1	ISO/IEC 27002:2022
MYCSC 17 - Incident response management			
17.1	PR.IP-9	12.10.3, 12.10.4	5.26 5.27
	DE.DP-1	N/A	
17.2	RS.CO-1	N/A	
17.3	PR.IP-9, PR.AT-1	12.10.1	
17.4	ID.GV-2, PR.IP-9, DE.DP-1, RS.CO-1	12.10.1	
17.5	DE.DP-4, RS.CO-2, RS.CO-3, RS.CO-4	N/A	
17.6	N/A	N/A	
17.7	PR.IP-10	N/A	
17.8	RS.IM-1, RS.IM-2	N/A	
17.9	RS.AN-4	N/A	
MYCSC 18 - Penetration testing			
18.1	PR.IP-7	11.3	8.8
18.2	N/A	11.3.1	
18.3	N/A	N/A	
18.4	N/A	N/A	
18.5	N/A	11.3.2	
MYCSC 19 - Threat intelligence			
19.1	N/A	N/A	5.7
MYCSC 20 - Information security for use of cloud services			
20.1	N/A	N/A	2.3
MYCSC 21 - Physical security monitoring			
21.1	N/A	N/A	7.4
MYCSC 22 - Information deletion			
22.1	N/A	N/A	8.10
MYCSC 23 - Data masking			
23.1	N/A	N/A	8.11
MYCSC 24 - Data leakage prevention			
24.1	N/A	N/A	8.12
MYCSC 25 - Web filtering			
25.1	N/A	N/A	8.22
MYCSC 26 - Secure coding			
26.1	N/A	N/A	8.28

Bibliography

[1] MCMC MTSFB TC G021, *Information and Network Security - Monitoring and Measurement of Security Control Objectives*

[2] ITU-T X Suppl. 36, *ITU-T X.1051 - Supplement on critical security controls for information and network security management by telecommunication organizations*

[3] ETSI TR 103 305-1, *CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls*

[4] NIST CSFv1.1, *Cybersecurity Framework Version 1.1*

[5] PCI DSS 3.2.1, *Understanding the Payment Card Industry Data Security Standard version 3.2.1*

Acknowledgements

Members of the Information and Network Security Sub Working Group

Ms Azrina Ibramsha (Chairman)	Telekom Malaysia Berhad
Ms Rafeah Omar (Vice Chairman)	Telekom Malaysia Berhad
Mr Thaib Mustafa (Draft lead)	FNS (M) Sdn Bhd
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Azlan Mohamed Ghazali	Deloitte Business Advisory Sdn Bhd
Mr Navinkumar Palani Velu	Digital Nasional Berhad
Ms Nur Amani Najwa Mohd Nazhir	FNS (M) Sdn Bhd
Mr Mohd Adlan Abd Wahab	Maxis Broadband Sdn Bhd
Mr Calvin Tan Tjin Wei/	U Mobile Sdn Bhd
Mr Robin Yong Hong Cheng	
Dr Ahmad Shahrafidz Khalid	Universiti Kuala Lumpur
Mr Mohd Hisyam Othman	Webe Digital Sdn Bhd

By invitation:

Mr Mohammad Zahir Mat Salleh	Celcom Axiata Berhad