Cyber Security Strategy

Table of Contents

[Executive Summary 3](#_Toc17202912)

[Purpose 4](#_Toc17202913)

[Objectives And Scope 4](#_Toc17202914)

[Approach 5](#_Toc17202915)

[Basic Controls 7](#_Toc17202916)

[**CIS Control 1: Inventory and Control of Hardware Assets** 7](#_Toc17202917)

[**CIS Control 2: Inventory and Control of Software Assets** 8](#_Toc17202918)

[**CIS Control 3: Continuous Vulnerability Management** 9](#_Toc17202919)

[**CIS Control 4: Controlled Use of Administrative Privileges** 10](#_Toc17202920)

[**CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers** 11](#_Toc17202921)

[**CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs** 12](#_Toc17202922)

[Foundation Controls 12](#_Toc17202923)

[**CIS Control 7: Email and Web Browser Protections** 12](#_Toc17202924)

[**CIS Control 8: Malware Defences** 12](#_Toc17202925)

[**CIS Control 9: Limitation and Control of Network Ports, Protocols and Services** 13](#_Toc17202926)

[**CIS Control 10: Data Recovery Capabilities** 13](#_Toc17202927)

[**CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches** 13](#_Toc17202928)

[**CIS Control 12: Boundry Defences** 13](#_Toc17202929)

[**CIS Control 13: Data Protection** 14](#_Toc17202930)

[**CIS Control 14: Controlled Access Based on the Need to Know** 14](#_Toc17202931)

[**CIS Control 15: Wireless Access Control** 14](#_Toc17202932)

[**CIS Control 16: Account Monitoring and Control** 14](#_Toc17202933)

[Organisational 15](#_Toc17202934)

[**CIS Control 17: Implement a Security Awareness and Training Program** 15](#_Toc17202935)

[**CIS Control 18: Application Software Security** 15](#_Toc17202936)

[**CIS Control 19: Incident Response Management** 15](#_Toc17202937)

[**CIS Control 20: Penetration Tests and Red Team Exercises** 16](#_Toc17202938)

[Roadmap 16](#_Toc17202939)

[Outcomes 17](#_Toc17202940)

[Definitions 17](#_Toc17202941)

# Executive Summary

**[An Overview Of What The Strategy Is For, What It Intends To Provide& How It Will Be Achieved.]**

The Cyber Security Strategy detailed in this document once executed will provide the required cyber security resilience so that **[Business Name]** will be able to execute the existing business plan and meet its key business objectives. This strategy includes establishing the strategic direction and the identification of key initiatives for cyber security at **[Business Name]** from 20XX until 20XX.

**Framework Adoption.**

As part of the development of this Cyber Security Strategy, **[Business Name]** has identified a number of risk reduction benefits and cost efficiencies that would be gained through the adoption of an established cyber security framework. The cost efficiencies are gained through the leveraging of a recognised industry body, that is more efficient than each company developing their own framework. Risk reduction benefits are gained through utilising a framework that has already been peer-reviewed and refined through the experience of its use in other organisations.

**CIS Controls.**

The CIS Controls have been developed by the Centre for Internet Security (CIS) It represents a prioritized set of actions that collectively form a defence in depth of “Best Practices” that mitigate the most common attacks against systems and networks. The CIS Controls overlay across other regulatory standards (PCI DSS, ISM, NIST, etc.) and can be adapted to regulatory standards as business requirements evolve.

**Recommendation**

It is recommended that **[Business Name]** adopt the CIS Controls as the guideline for the Cyber Security Strategy. It would be recommended that **[Business Name]** adopt CIS Controls even if there is not an anticipated future regulatory requirement as it offers **[Business Name]** the most cost effective and risk effective standards basis for its Cyber Security Strategy. It will assist with building a solid cyber security foundation and culture that will enable **[Business Name]** to safely and securely meet its business objectives.

# Purpose

**[Describe What The Intent Of This Document Will Be.]**

This document sets forth the Cyber Security Strategy for **[Business Name]**. It establishes the business direction and guidelines for consistency and compliance in executing the **[Business Name]** Cyber Security Strategy

# Objectives And Scope

The overall objective for **[Business Name]** is to increase resilience, visibility, capability, maturity and continuity by taking a risk-based approach to cyber security and allow **[Business Name]** to safely and securely meet its business objectives.

The adoption of a risk-based approach to security provides aligns with the current corporate business strategy and allows for **[Business Name]** to utilise the same methodology across business units to embed security in to the organisation and foster a security aware culture.

To ensure this, **[Business Name]** cyber security strategy is developed to, and maintained at, a maturity level that:

* Is commensurate with the risk profile of the organisation
* Enables compliance with relevant legislation and regulation
* Provides better alignment to business initiatives
* provides visibility of risk profile across the organisation

Cyber Security should be viewed as a journey which involves the entire organisation and as business units become “Security Aware” the maturity of **[Business Name]** will begin to improve.

**[Business Name]** has already made a range of improvements to cyber security, including;

**[List Some Of The Security Controls & Projects That Have Been Implemented.]**

While these improvements have been successful, the overall approached has been developed in a somewhat piecemeal manner and has lacked any overarching strategy or target state.

To ensure **[Business Name]** to safely and securely meet its business objectives, the strategy incorporates cyber security, disaster recovery and business continuity. The scope of the strategy will focus on systems and processes that support business-critical functions that will enable **[Business Name]** to safely and securely meet its business objectives. These systems include;

* Corporate IT systems (e.g. corporate and guest network domains, applications)
* All users of the above systems (e.g. employees, contractors and visitors)
* All providers of IT goods and services
* All locations from which the organisation conducts business operations
* All participants in the supply chain

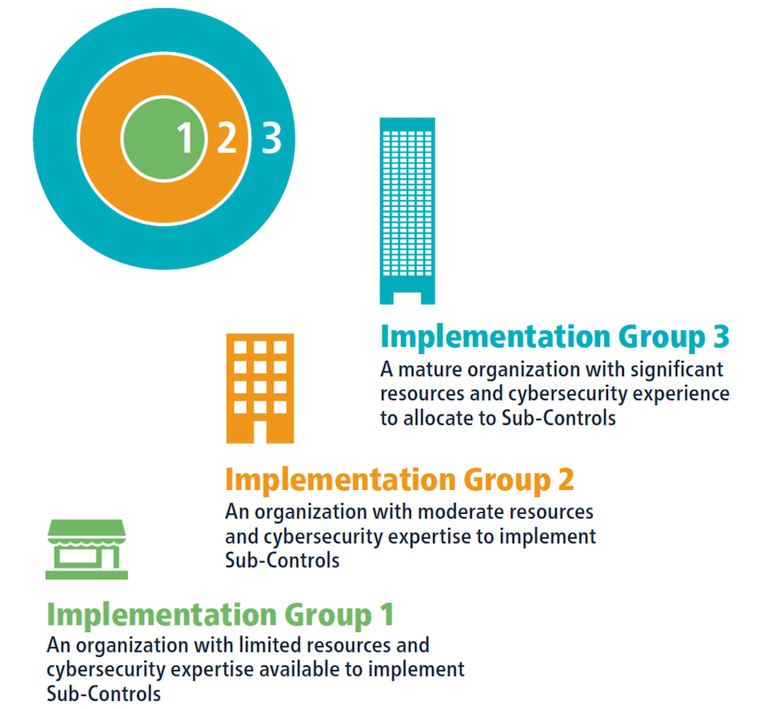
# Approach

In order to provide a structured approach to Cyber Security, **[Business Name]** have chosen to align to the CIS Controls. The CIS Controls will enable **[Business Name]**to utilise this framework to implement security initiatives in a structured manner and provide a solid foundation in which to build upon.

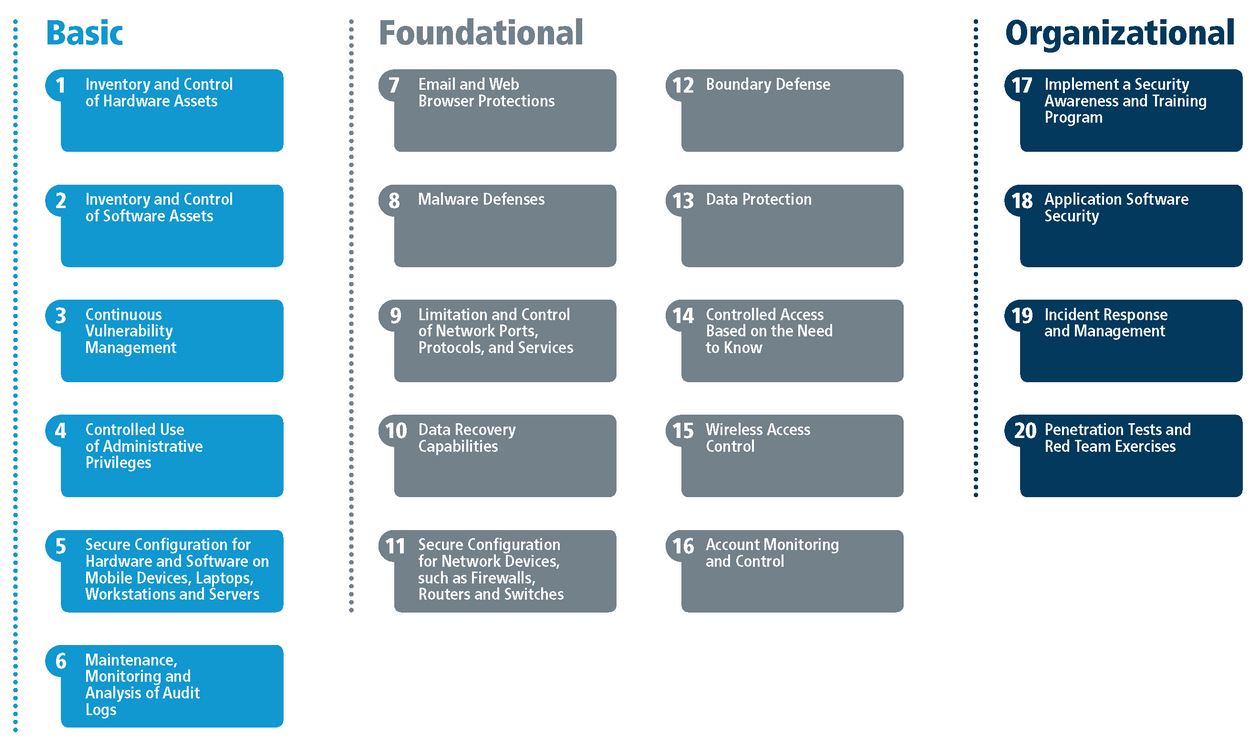
The CIS Controls are broken up in to three categories. **Basic**, **Foundational** and **Organisational.** Historically the CIS Controls utilised the order of the Controls as a means of focusing an organization’s cybersecurity activities, resulting in a subset of the first six CIS Controls referred to as cyber hygiene. However, many of the practices found within the CIS cyber hygiene control set can be difficult for organisations with limited resources to implement.

This highlighted a need for a collection of best practices focused on balancing resource constraints and effective risk mitigation. As a result, CIS recommends the following new guidance to prioritise CIS Control utilisation, known as CIS Controls Implementation Groups (IG). The IG groups are broken down in to three groups and are determined based on resource availability, budget and capability.

**[Business Name]** will undertake alignment to CIS Controls by implementing the controls outlined within Implementation Group 1. This approach will provide a solid foundation in which to build upon and once completed, **[Business Name]** will begin implementing the controls outlined within Implementation Group 2 and then Implementation Group 3.



The below diagram highlights the journey **[Business Name]** will need to undertake and the core components of the CIS Controls which align to with the objective to move from its “current state” to its “desired state”

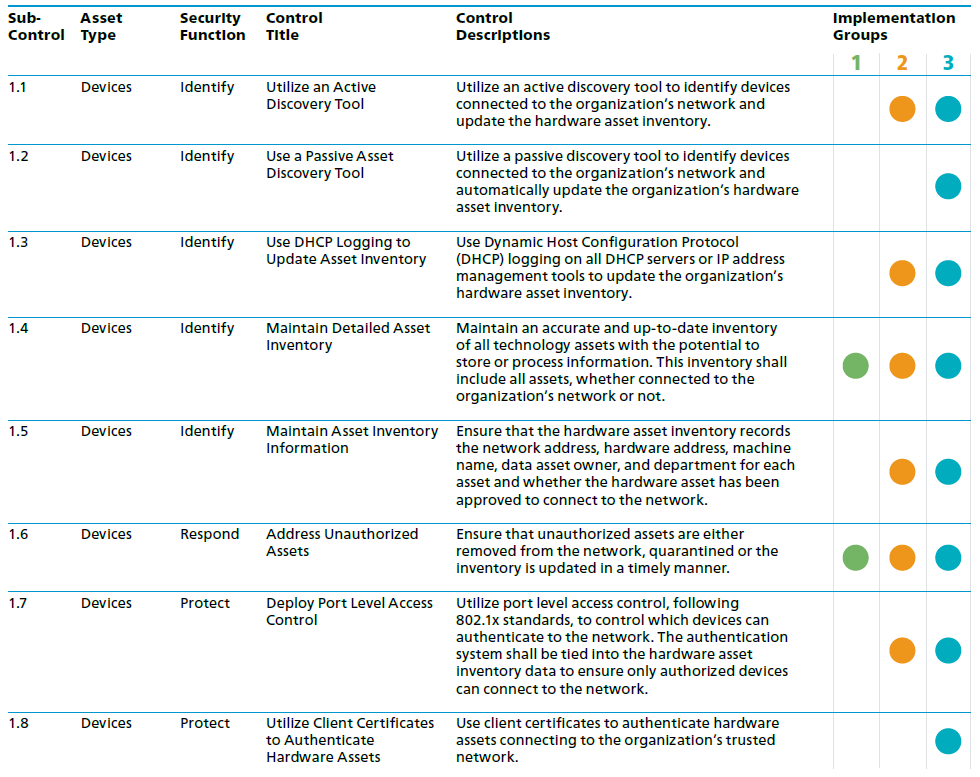


## Basic Controls

### **CIS Control 1: Inventory and Control of Hardware Assets**

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.

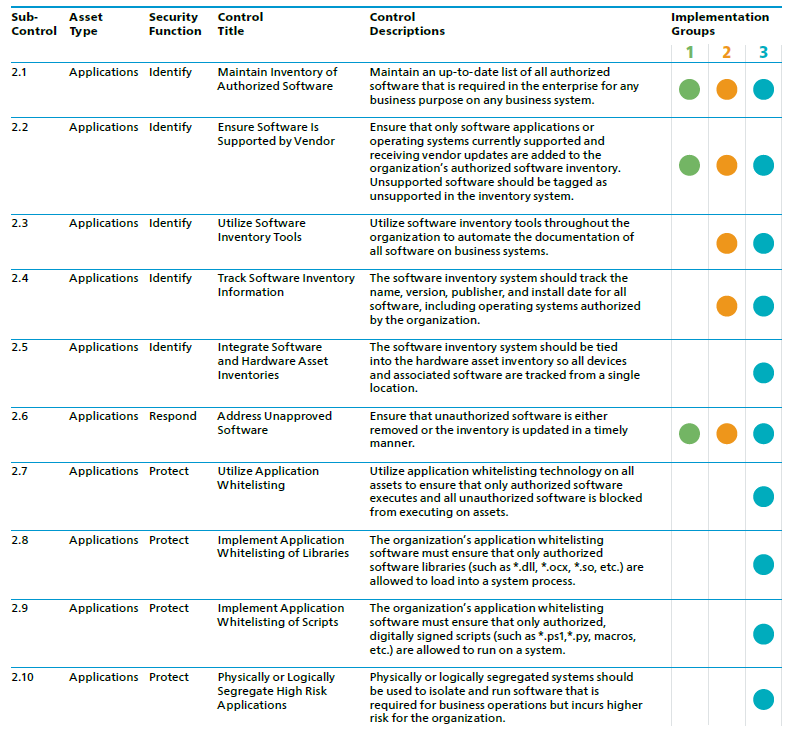
**[Business Name]** will initially implement IG1 sub-control 1.4 and 1.6



### **CIS Control 2: Inventory and Control of Software Assets**

Actively manage (inventory, track, and correct) all software on the network so that only authorised software is installed and can execute, and that all unauthorised and unmanaged software is found and prevented from installation or execution.

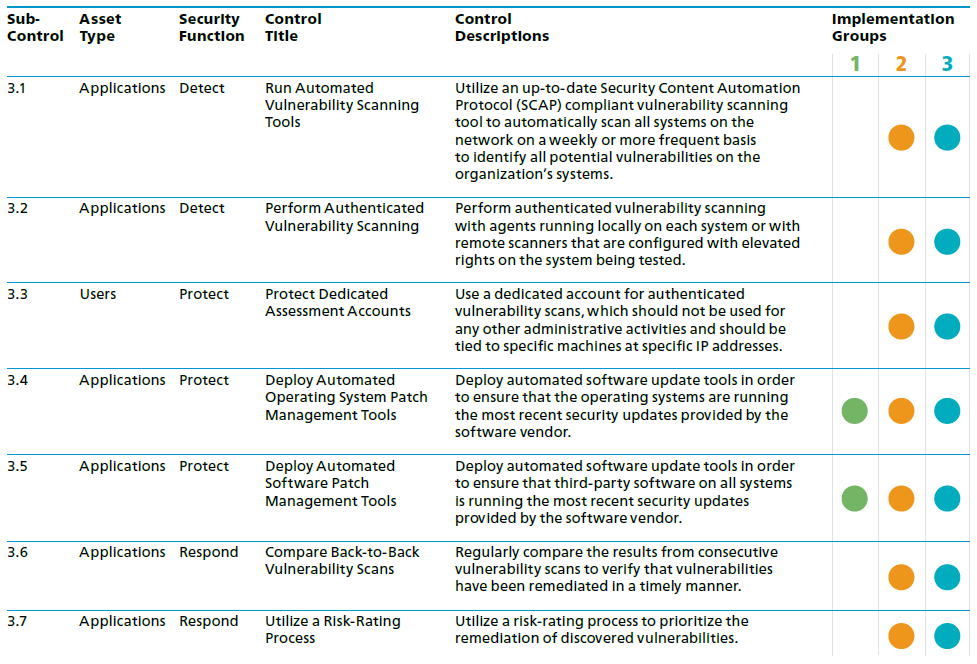
**[Business Name]** will initially implement IG1 sub-control 2.1, 2.2 and 2.6



### **CIS Control 3: Continuous Vulnerability Management**

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimise the window of opportunity for attackers.

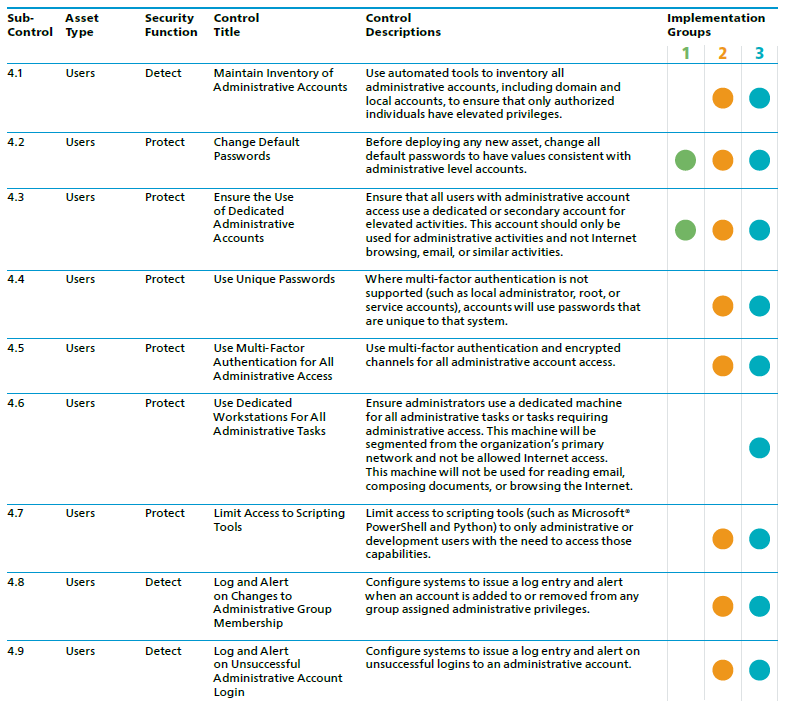
**[Business Name]** will initially implement IG1 sub-control 3.4 and 3.5



### **CIS Control 4: Controlled Use of Administrative Privileges**

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

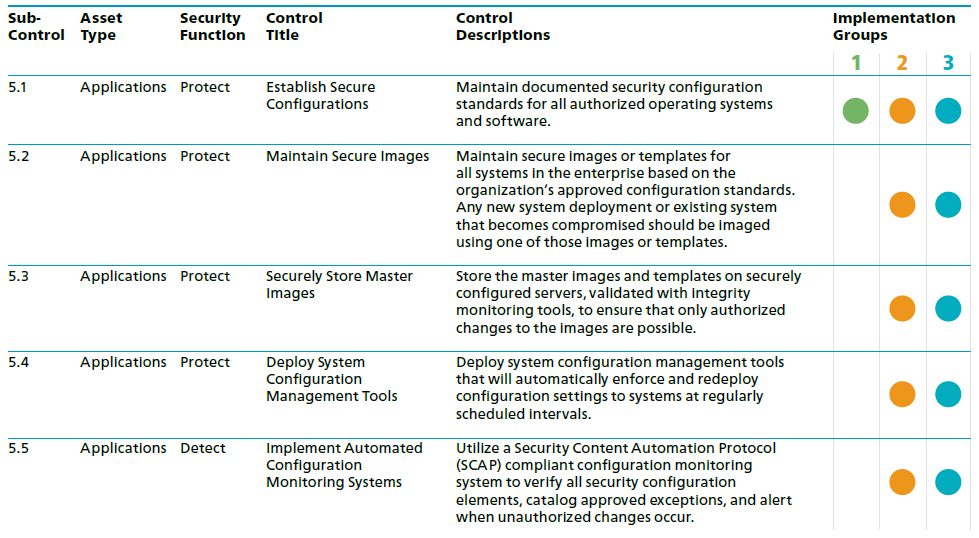
**[Business Name]** will initially implement IG1 sub-control 4.2 and 4.3



### **CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

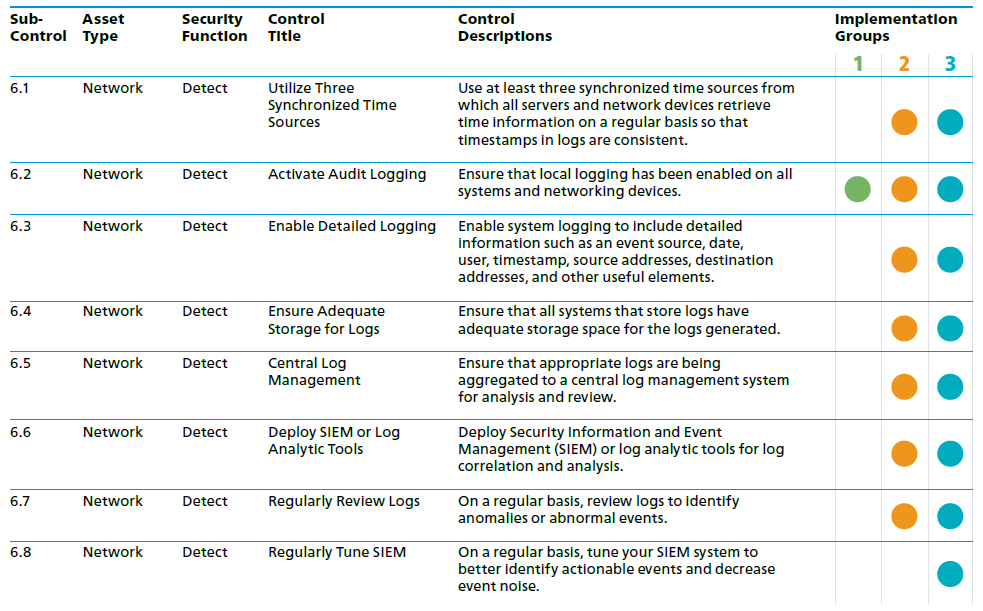
**[Business Name]** will initially implement IG1 sub-control 5.1



### **CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs**

Collect, manage, and analyse audit logs of events that could help detect, understand, or recover from an attack.

**[Business Name]** will initially implement IG1 sub-control 6.2



## Foundation Controls

### **CIS Control 7: Email and Web Browser Protections**

Minimise the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

**[Business Name]** will initially implement IG1 sub-control:

* 7.1 - Ensure that only fully supported web browsers and email clients are allowed to execute in the organisation, ideally only using the latest version of the browsers and email clients provided by the vendor.
* 7.7 - Use Domain Name System (DNS) filtering services to help block access to known malicious domains.

### **CIS Control 8: Malware Defences**

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.

**[Business Name]** will initially implement IG1 sub-control:

* 8.2 - Ensure that the organization’s anti-malware software updates its scanning engine and signature database on a regular basis.
* 8.4 - Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
* 8.5 - Configure devices to not auto-run content from removable media.

### **CIS Control 9: Limitation and Control of Network Ports, Protocols and Services**

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimise windows of vulnerability available to attackers

**[Business Name]** will initially implement IG1 sub-control:

* 9.4 - Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

### **CIS Control 10: Data Recovery Capabilities**

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

**[Business Name]** will initially implement IG1 sub-control:

* 10.1 - Ensure that all system data is automatically backed up on a regular basis.
* 10.2 - Ensure that all of the organisation’s key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
* 10.4 - Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
* 10.5 - Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

### **CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches**

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

**[Business Name]** will initially implement IG1 sub-control:

* 11.4 - Install the latest stable version of any security related updates on all network devices.

### **CIS Control 12: Boundry Defences**

Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

**[Business Name]** will initially implement IG1 sub-control:

* 12.1 – Maintain an up-to-date inventory of all of the organisation’s network boundaries.
* 12.4 - Deny communication over unauthorised TCP or UDP ports or application traffic to ensure that only authorised protocols are allowed to cross the network boundary in or out of the network at each of the organisation’s network boundaries.

### **CIS Control 13: Data Protection**

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

**[Business Name]** will initially implement IG1 sub-control:

* 13.1 – Maintain an inventory of all sensitive information stored, processed, or transmitted by the organisation’s technology systems, including those located on-site or at a remote service provider.
* 13.2 – Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
* 13.6 – Utilise approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.

### **CIS Control 14: Controlled Access Based on the Need to Know**

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

**[Business Name]** will initially implement IG1 sub-control:

* 14.6 - Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorised individuals should have access to the information based on their need to access the information as a part of their responsibilities.

### **CIS Control 15: Wireless Access Control**

The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

**[Business Name]** will initially implement IG1 sub-control:

* 15.7 - Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
* 15.10 - Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.

### **CIS Control 16: Account Monitoring and Control**

Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimise opportunities for attackers to leverage them.

**[Business Name]** will initially implement IG1 sub-control:

* 16.8 – Disable any account that cannot be associated with a business process or business owner.
* 16.9 – Automatically disable dormant accounts after a set period of inactivity.
* 16.11 - Automatically lock workstation sessions after a standard period of inactivity.

# Organisational

### **CIS Control 17: Implement a Security Awareness and Training Program**

For all functional roles in the organisation (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programs.

**[Business Name]** will initially implement IG1 sub-control:

* 17.3 – Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organisation’s security awareness program should be communicated in a continuous and engaging manner.
* 17.5 – Train workforce members on the importance of enabling and utilising secure authentication.
* 17.6 – Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
* 17.7 – Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.
* 17.8 – Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.
* 17.9 – Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.

### **CIS Control 18: Application Software Security**

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

**[Business Name]** will initially implement IG1 sub-control:

The CIS Controls does not specify any IG1 controls to be implemented

### **CIS Control 19: Incident Response Management**

Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.

**[Business Name]** will initially implement IG1 sub-control:

* 19.1 – Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.
* 19.3 – Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.
* 19.5 – Assemble and maintain information on thirdparty contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.
* 19.6 – Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.

### **CIS Control 20: Penetration Tests and Red Team Exercises**

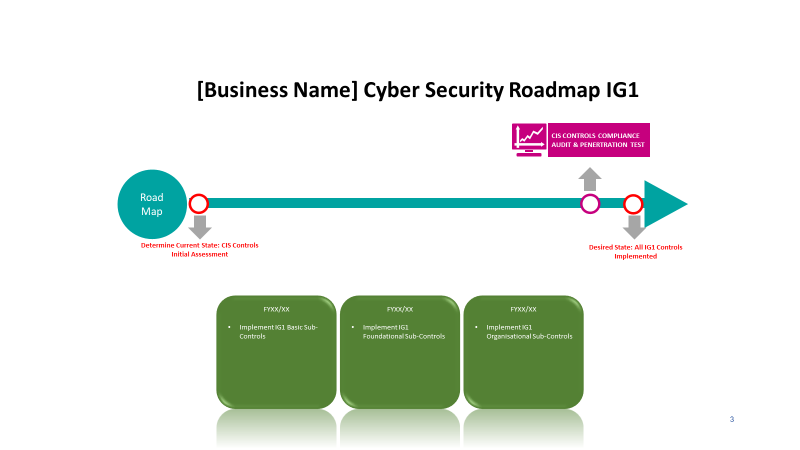
Test the overall strength of an organization’s defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

**[Business Name]** will initially implement IG1 sub-control:

The CIS Controls does not specify any IG1 controls to be implemented

# Roadmap

In order to meet the objectives and improve maturity, a roadmap has been developed to assist with prioritisation of initiatives. The roadmap below provides an overview of the security initiatives which will contribute to the alignment with the CIS Controls and improving the maturity of Cyber Security for **[Business Name]**



**[Insert A Copy Of The Roadmap.]**

# Outcomes

The success of the strategy can be measured through the use of the CIS Controls Assessment Tool (CAT) The CAT is directly aligned to the CIS Controls and will enable **[Business Name]** to measure, manage and track progress of security initiatives to ensure that all applicable requirements are compliant.

A CAT gap analyses will be developed as the first components to understand the current state of **[Business Name]** and what controls have already been met. A list of project initiatives can then be developed to enable **[Business Name]** to deliver on the outcomes outlined in the strategy and improve the maturity of the organisation.

Several high-level outcomes are expected to be delivered which include but are not limited to;

* The Strategy Developed and Communicated
* Policies and Procedures Operationalised
* Resources (Financial and Human) Identified and Allocated
* Technologies Selected and Implemented
* Employees Educated and Committed
* Ongoing Monitoring, Evaluation and Improvement in Place

# Definitions

**[Define Any Terms That Are Used Throughout This Document.]**

|  |  |
| --- | --- |
| Terms | Definition |
| IT Asset | **IT Asset** refers to anything (tangible or intangible) that has value to an organisation, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualised computing), and related hardware (e.g., locks, cabinets, keyboards), as well as people and intellectual property (including software). |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |