A School Board Perspective on Cyber Risk - What Boards Look For When Approving Cyber Security Budgets

9:10am - 9:50am

John Baird, Cyber Security Advisory Board, Australian Computer Society

A School Board perspective on Cyber Risk

What Boards Look For When Approving Cyber Security Budgets

A School Board perspective on Cyber Risk

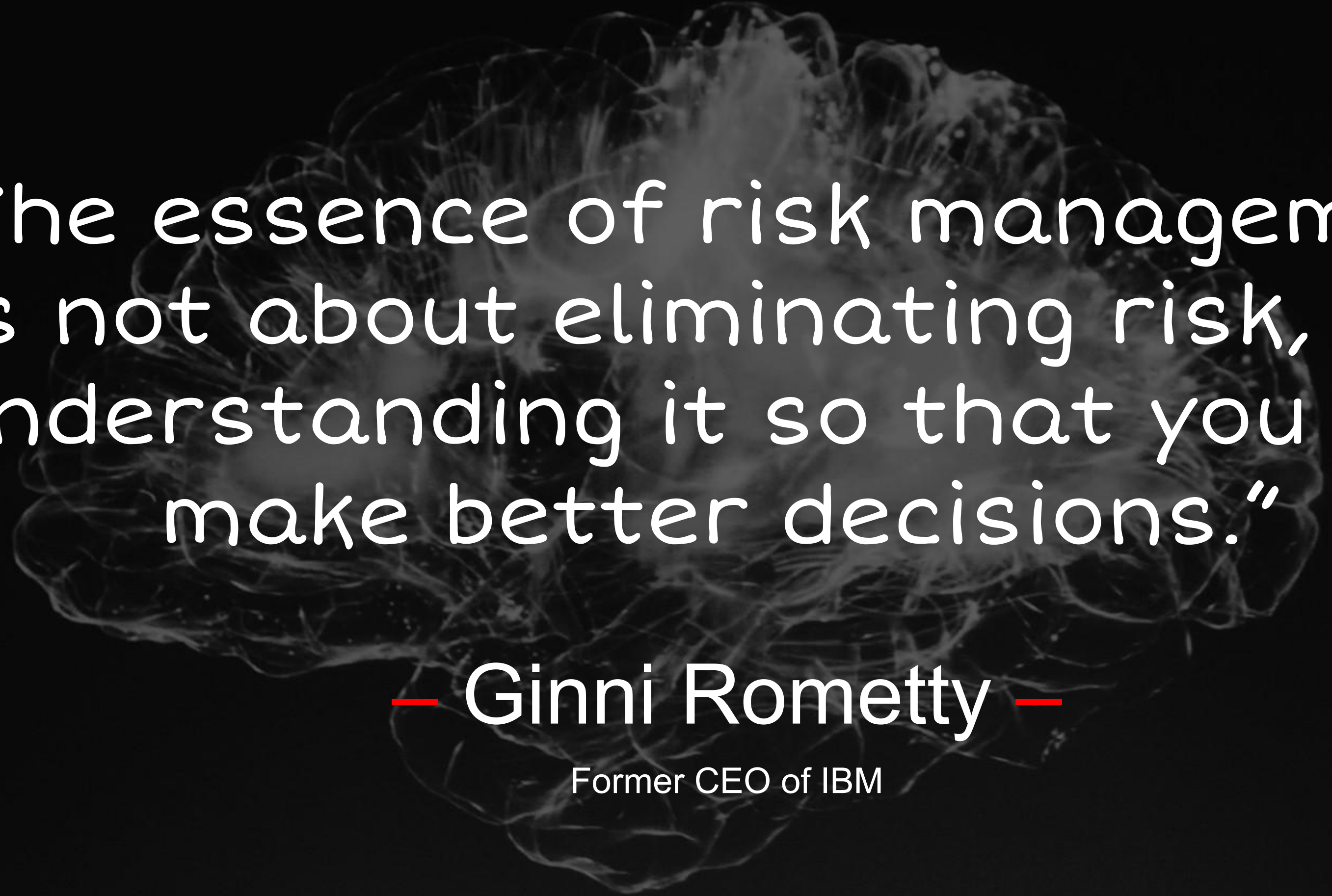
What Boards Look For When Approving Cyber Security Budgets

Or

Why won’t they just give me the money?

01

Bridging the gap



“The essence of risk management is not about eliminating risk, but understanding it so that you can make better decisions.“

– Ginni Rometty –

Former CEO of IBM

Bridging the Gap

Bridging the Gap

School board members make big-picture decisions that shape the future of education in their community. They should always focus on what’s best for students while being mindful of financial constraints and community expectations.

Bridging the Gap

A School IT Manager is crucial in ensuring that technology supports education, operations, and security within a school or district. Without a skilled IT Manager, schools risk downtime, security breaches, and ineffective technology use, which can negatively impact learning and operations. They ensure that technology enhances education rather than becoming a barrier.

Bridging the Gap

School board members make big-picture decisions that shape the future of education in their community. They should always focus on what’s best for students while being mindful of financial constraints and community expectations.

A School IT Manager is crucial in ensuring that technology supports education, operations, and security within a school or district. Without a skilled IT Manager, schools risk downtime, security breaches, and ineffective technology use, which can negatively impact learning and operations. They ensure that technology enhances education rather than becoming a barrier.

Bridging the Gap

School board members look to quantify and manage risks.

A School IT Manager seeks to eliminate risk.

Bridging the Gap

Common Approach

Common Language

Bridging the Gap

Common Approach

IT managers must adopt a risk-based approach, framing cybersecurity not as a list of technical tasks but as a strategic decision-making process. By assessing, prioritising, and communicating risks in business terms, they can ensure leadership understands the real impact of security choices.

Common Language

Bridging the Gap

Common Approach

IT managers must adopt a risk-based approach, framing cybersecurity not as a list of technical tasks but as a strategic decision-making process. By assessing, prioritising, and communicating risks in business terms, they can ensure leadership understands the real impact of security choices.

Common Language

To bridge the gap between IT teams and school boards, you need a common language—one that translates technical cybersecurity concerns into business risks and organisational priorities. Without this shared understanding, critical security needs can be overlooked or dismissed.

Bridging the Gap

Common Understanding

In risk language, a penetration test should be framed as a **preventative control** that helps reduce the **likelihood and impact** of cybersecurity threats. Organisations face **continuous threats** from cybercriminals, insider threats, and evolving attack techniques—without regular testing, vulnerabilities may go undetected, increasing the **risk of financial loss, reputational damage, and regulatory penalties**. By simulating real-world attacks, penetration tests provide **actionable insights** into security weaknesses, enabling businesses to make informed decisions about **risk treatment** strategies, such as remediation, mitigation, or acceptance. Ultimately, penetration testing is not just a compliance requirement but a **critical risk management practice** that ensures cybersecurity defences are aligned with **business risk tolerance** and evolving threat landscapes.

Bridging the Gap

Common Understanding

In risk language, a penetration test should be framed as a **preventative control** that helps reduce the **likelihood and impact** of cybersecurity threats. Organisations face **continuous threats** from cybercriminals, insider threats, and evolving attack techniques—without regular testing, vulnerabilities may go undetected, increasing the **risk of financial loss, reputational damage, and regulatory penalties**. By simulating real-world attacks, penetration tests provide **actionable insights** into security weaknesses, enabling businesses to make informed decisions about **risk treatment** strategies, such as remediation, mitigation, or acceptance. Ultimately, penetration testing is not just a compliance requirement but a **critical risk management practice** that ensures cybersecurity defences are aligned with **business risk tolerance** and evolving threat landscapes.

Uncovering the risk landscape

Risks can go on forever…

Cybersecurity risks are endless, from cyberattacks to human errors and system flaws.

While no single solution can stop them all, a strong **framework** helps you uncover the risks that you need to address.

03

Frameworks

Technology is not the (only) answer

“"It is the framework which changes with each new technology and not just the picture within the frame.

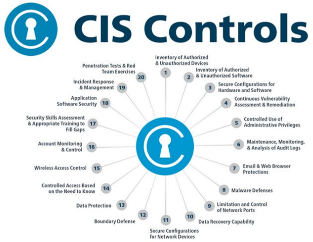
- Marshall McLuhan -

Canadian philosopher.

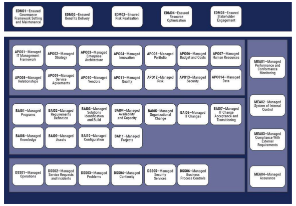
Frameworks

Security Frameworks

Planning for such a potentially complex and overwhelming situation is no trivial task. There are well-established frameworks developed by government agencies and industry bodies, such as NIST, SANS and the ACSC, to assist organisations in developing best practice response capabilities. Most organisations start with one of these and then augment it with their specific requirements.


CIS Controls
1 Inventory of Authorized & Unauthorized Devices
2 Inventory of Authorized & Unauthorized Software
3 Secure Configurations for Hardware and Software
4 Continuous Vulnerability Assessment & Remediation
5 Controlled Use of Administrative Privileges
6 Maintenance, Monitoring, & Analysis of Audit Logs
7 Email & Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports
10 Data Recovery Capability
11 Secure Configurations for Network Devices
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring & Control
17 Security Skills Assessment & Appropriate Training to Fill Gaps
18 Application Software Security
19 Incident Response & Management
20 Penetration Tests & Red Team Exercises

Information Security Management
ISO
27001
Certified

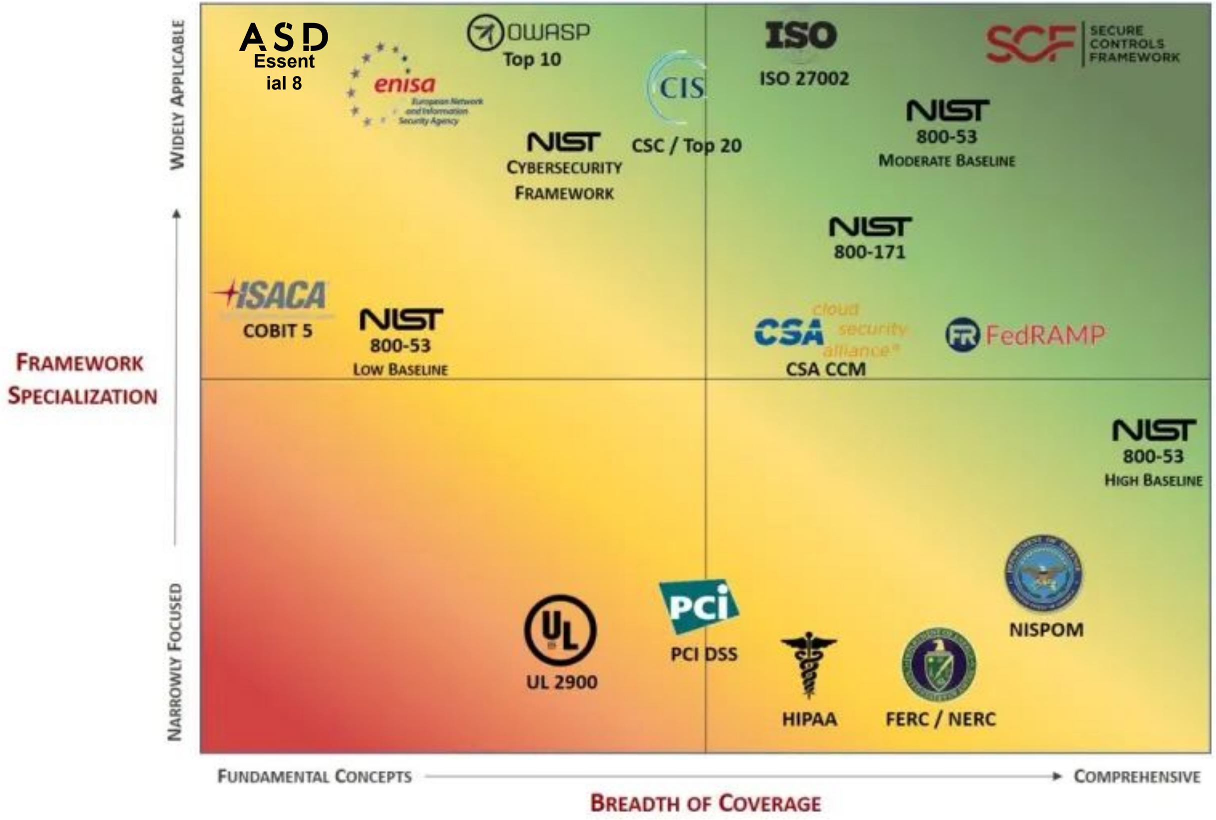

EDM01—Ensured Governance Framework Setting and Maintenance
EDM02—Ensured Benefits Delivery
EDM03—Ensured Risk Realization
EDM04—Ensured Resource Optimization
EDM05—Ensured Stakeholder Engagement
APO01—Managed IT Management Framework
APO02—Managed Strategy
APO03—Managed Enterprise Architecture
APO04—Managed Innovation
APO05—Managed Portfolio
APO06—Managed Budget and Costs
APO07—Managed Human Resources
APO08—Managed Relationships
APO09—Managed Service Agreements
APO10—Managed Vendors
APO11—Managed Quality
APO12—Managed Risk
APO13—Managed Security
APO014—Managed Data
BAI01—Managed Programs
BAI02—Managed Requirements Definition
BAI03—Managed Solutions Identification and Build
BAI04—Managed Availability and Capacity
BAI05—Managed Organizational Change
BAI06—Managed IT Changes
BAI07—Managed IT Change Acceptance and Transitioning
BAI08—Managed Knowledge
BAI09—Managed Assets
BAI10—Managed Configuration
BAI11—Managed Projects
DSS01—Managed Operations
DSS02—Managed Service Requests and Incidents
DSS03—Managed Problems
DSS04—Managed Continuity
DSS05—Managed Security Services
DSS06—Managed Business Process Controls
MEA01—Managed Performance and Conformance Monitoring
MEA02—Managed System of Internal Control
MEA03—Managed Compliance With External Requirements
MEA04—Managed Assurance

COBIT 2019

ACSC Australian Cyber Security Centre

NIST
National Institute of Standards and Technology
SP 800-82 Rev. 2

Frameworks



Protecting what matters most
Revio Cyber Security

Frameworks

Aspect	Essential 8	NIST	CIS
Number of Controls	8	23	18
Security Levels	4 (ML0 to ML3)	Risk Based	3 (IG1 – IG3)
Total points of control	50+	108+	150+
Focus	Risk mitigation through 8 key strategies	Comprehensive security covering identification, protection, detection, response, and recovery	Comprehensive security across 18 categories
Best for	Australian organisations & compliance with ASD	Global standard, risk-based security strategy	Global standard, broader industry adoption

Preparing the organisation

Security Frameworks

These security frameworks define policies and procedures for establishing and maintaining security controls. The frameworks clarify the processes used to protect an organization from cybersecurity risks.

Preparing the organisation

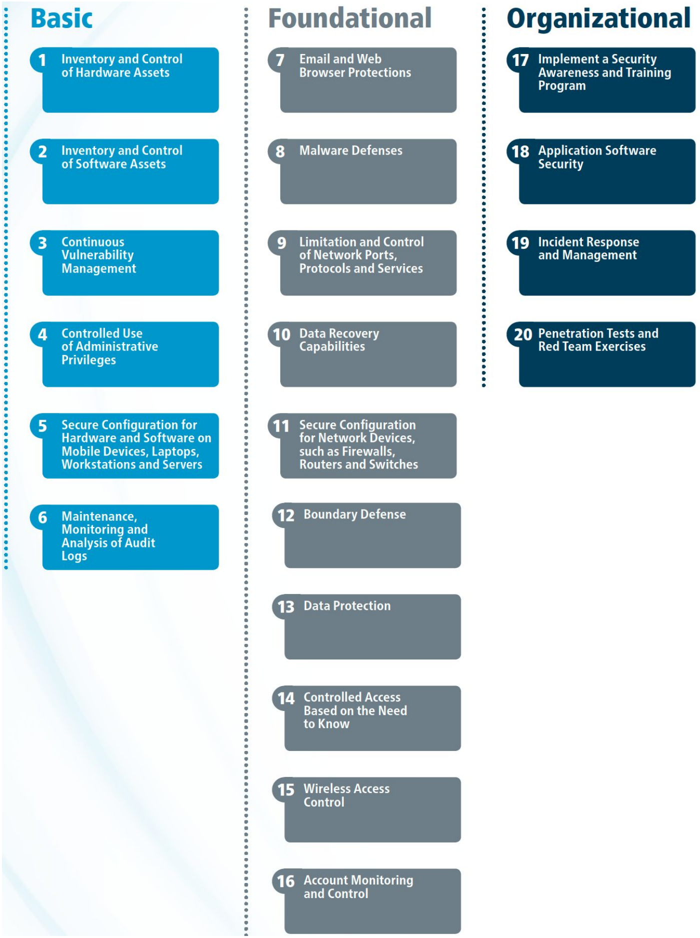
CIS Critical Security Controls

A prioritized set of actions to protect an organization and its data from cyber-attack vectors.

CIS. Center for Internet Security®

Creating Confidence in the Connected World.™

Preparing the organisation



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

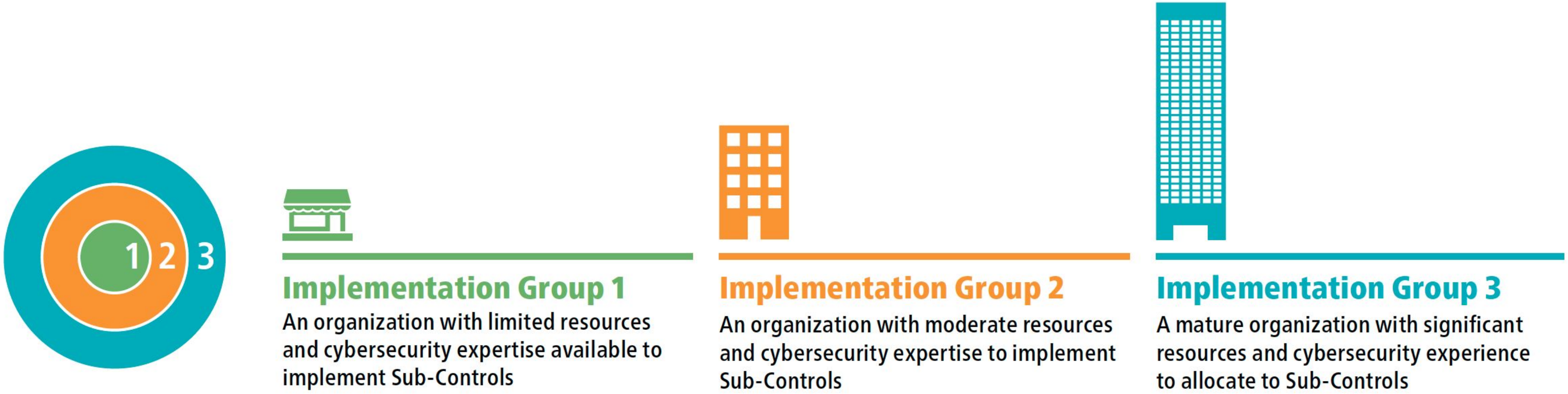
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Preparing the organisation

CIS Controls

The CIS controls can be implemented at three levels of maturity depending upon the readiness of the company implementing them.



Implementation Group 1

An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

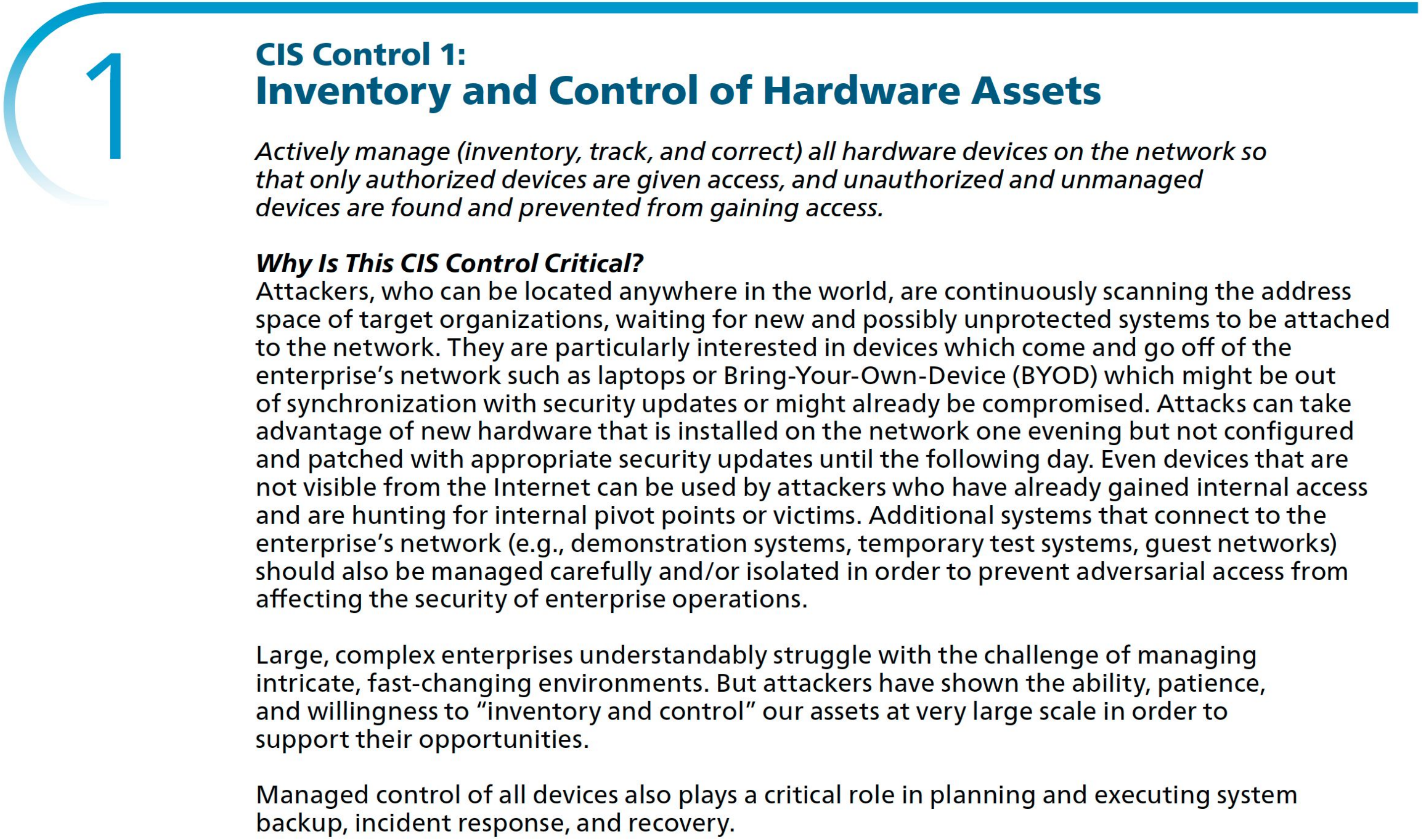
Implementation Group 2

An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 3

A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Preparing the organisation



1

CIS Control 1:
Inventory and Control of Hardware Assets

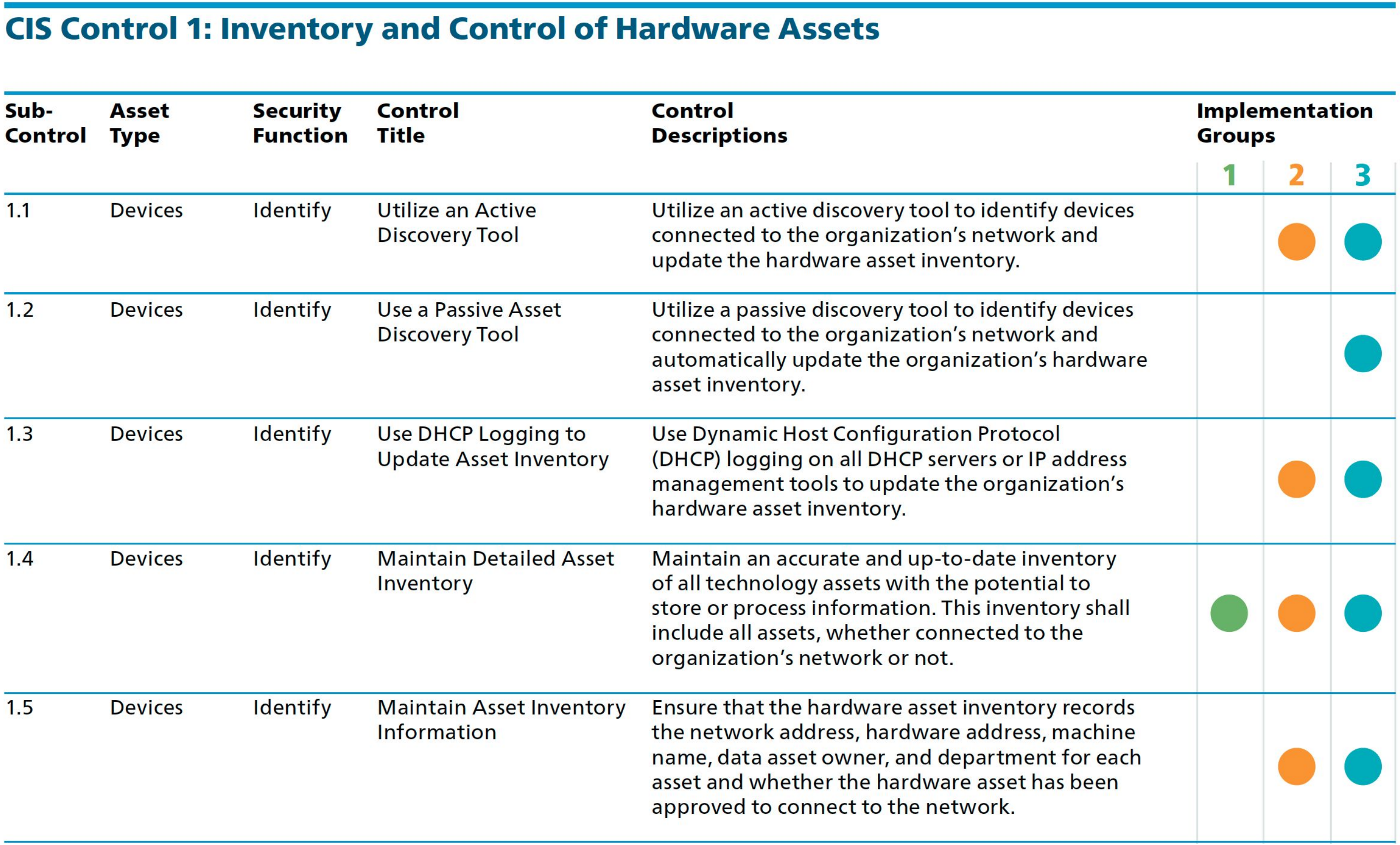
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This CIS Control Critical?
Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise’s network such as laptops or Bring-Your-Own-Device (BYOD) which might be out of synchronization with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise’s network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. But attackers have shown the ability, patience, and willingness to “inventory and control” our assets at very large scale in order to support their opportunities.

Managed control of all devices also plays a critical role in planning and executing system backup, incident response, and recovery.

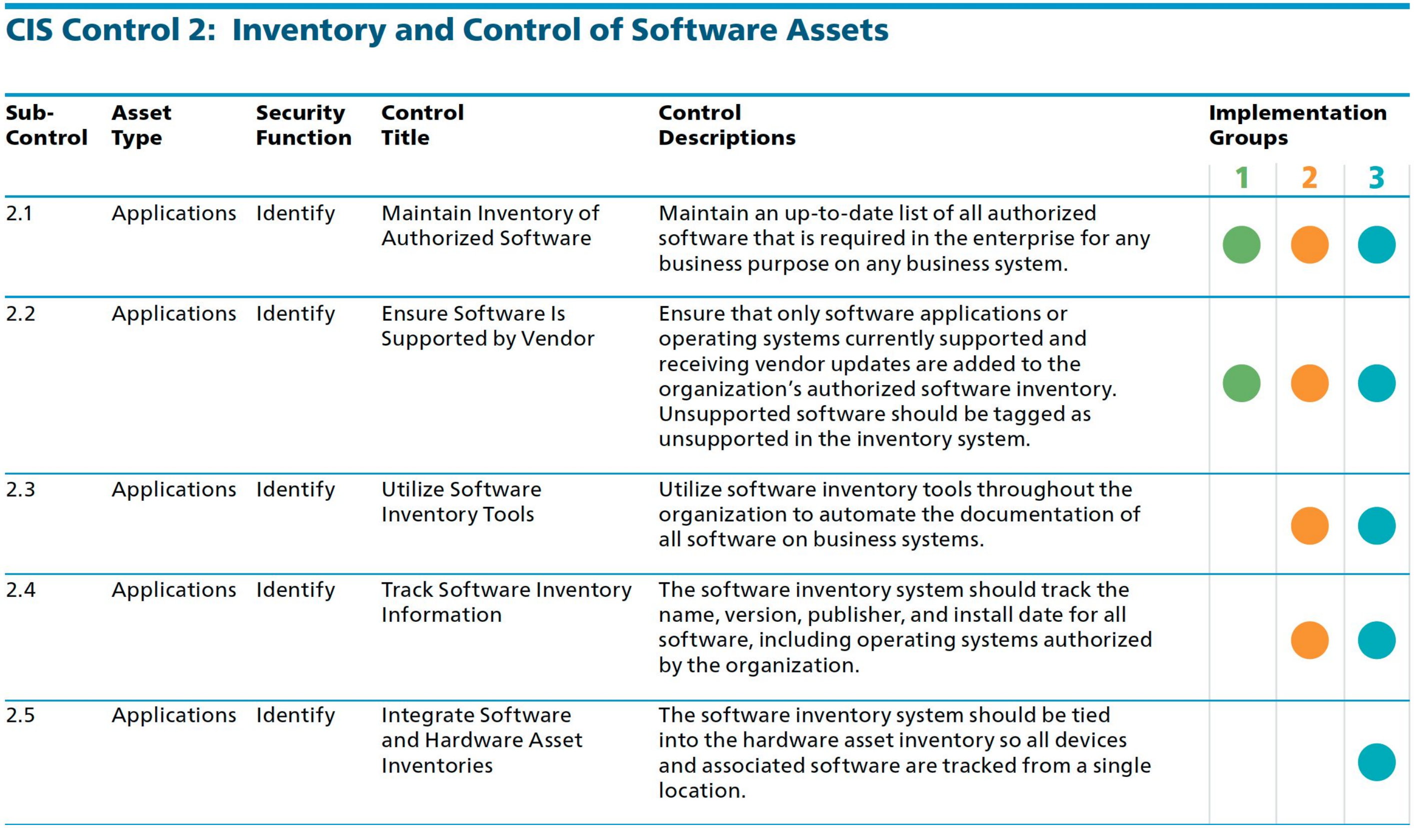
Preparing the organisation



CIS Control 1: Inventory and Control of Hardware Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		●	●
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			●
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		●	●
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	●	●	●
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		●	●

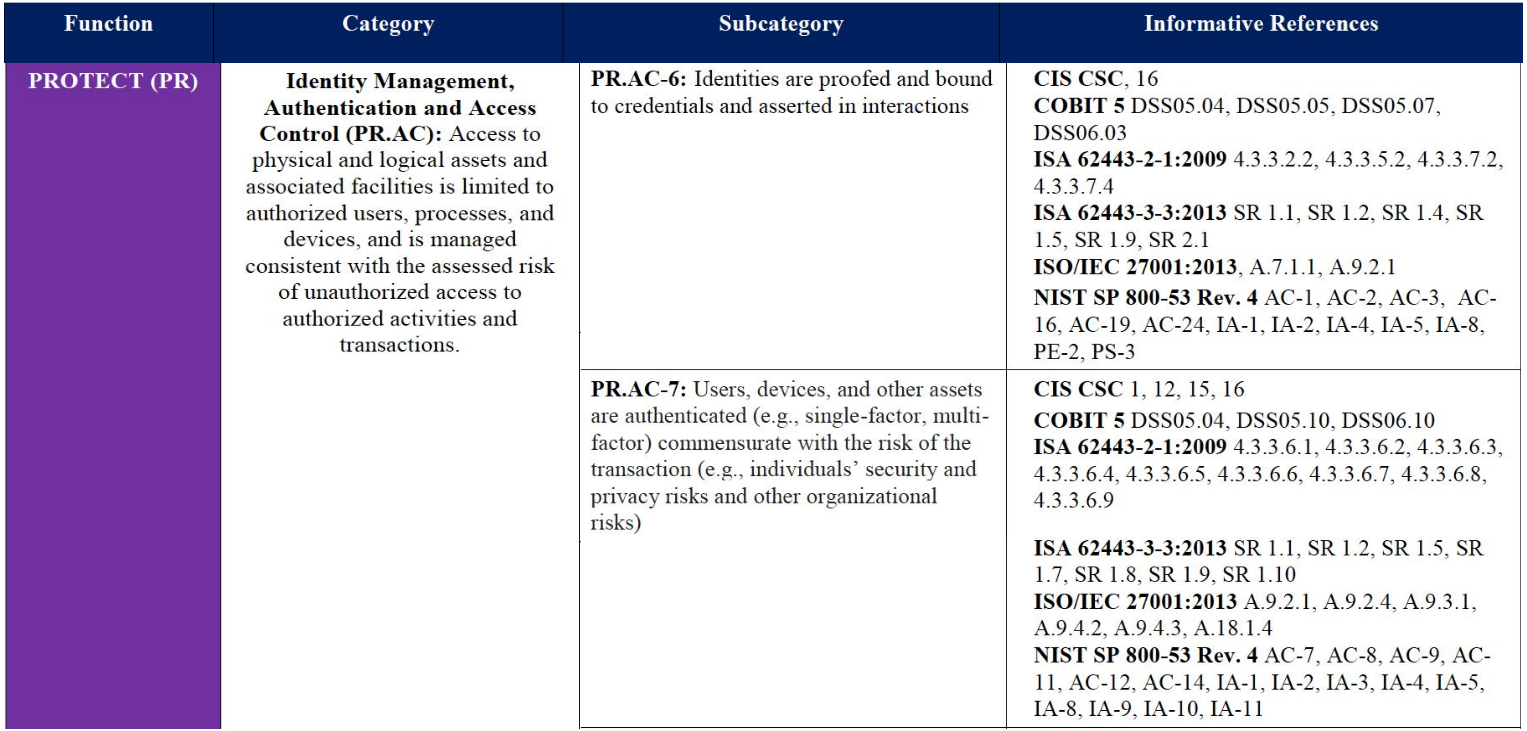
Preparing the organisation



CIS Control 2: Inventory and Control of Software Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	●	●	●
2.2	Applications	Identify	Ensure Software Is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization’s authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●
2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.		●	●
2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.		●	●
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			●

Preparing the organisation



Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions

23 Categories

108 Subcategories

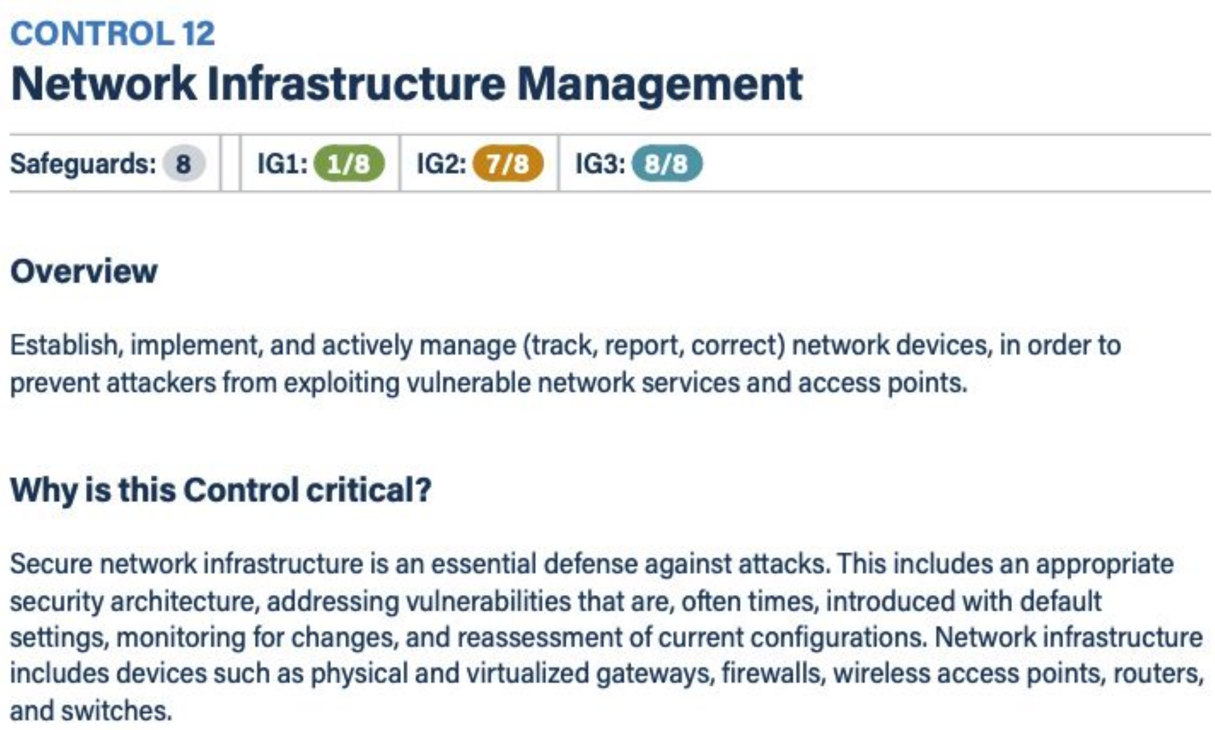
6 Informative References

Preparing the organisation

Australian Cyber Security Centre

The Essential Eight is a series of baseline mitigation strategies taken from the Strategies to Mitigate Cyber Security Incidents recommended for organisations. Implementing these strategies as a minimum makes it much harder for adversaries to compromise systems.

A sample control from CISv8.1



CONTROL 12

Network Infrastructure Management

Safeguards: 8	IG1: 1/8	IG2: 7/8	IG3: 8/8

Overview

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

Why is this Control critical?

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

Bridging the Gap

Common Understanding

Once a framework is selected, it is crucial to express each control using risk language.

Identify the type of control: **preventative, detective or reactive**

Calculate the **likelihood** and **impact** of a risk happening

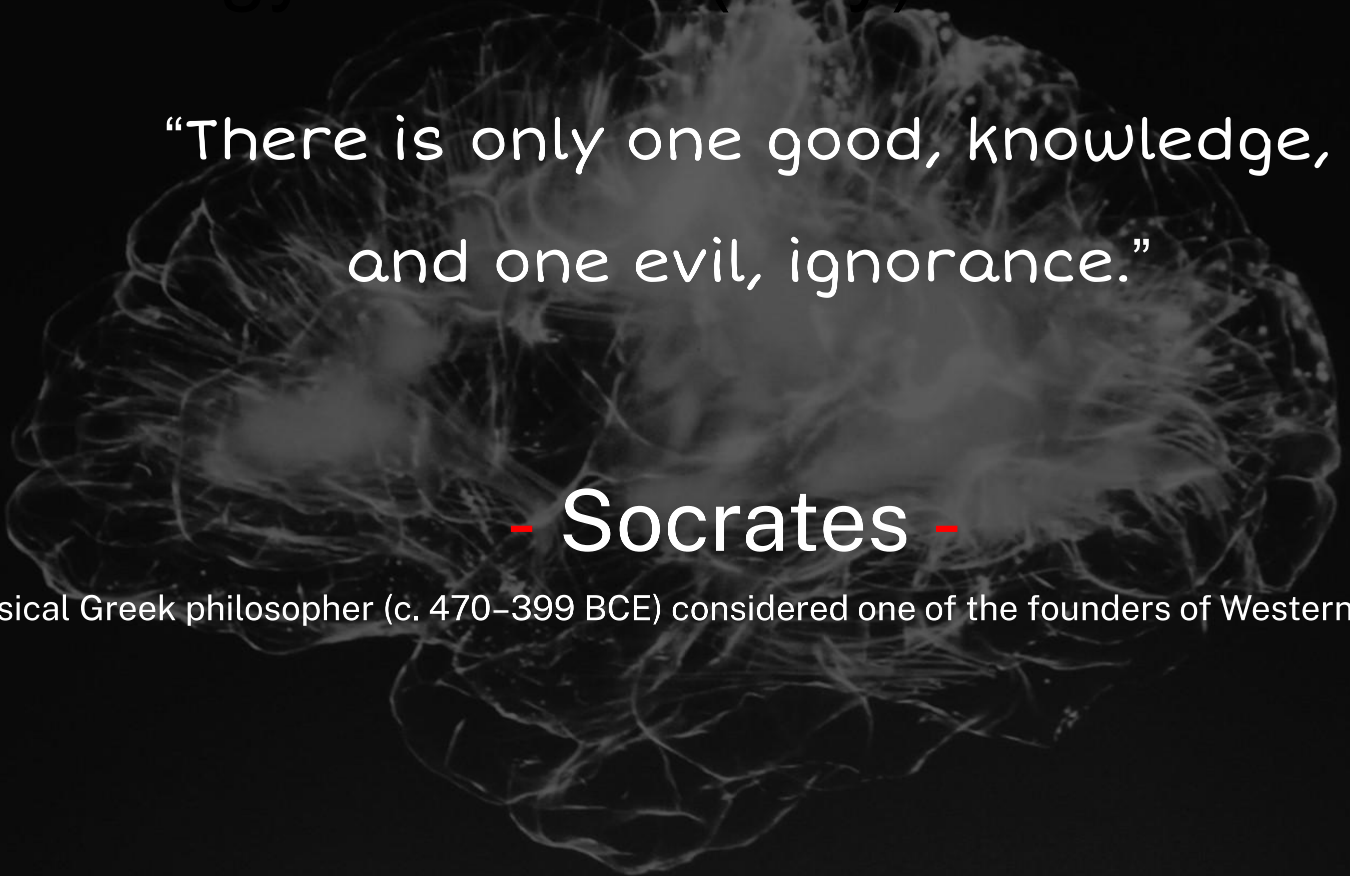
Identify the kind of impact: **financial loss, reputational damage, or regulatory penalties**.

Explain your plan **risk treatment**, such as remediation, mitigation, or acceptance.

Document and get agreement on the **residual risk**

Making a plan

Technology is not the (only) answer



“There is only one good, knowledge,

and one evil, ignorance.”

- Socrates -

Classical Greek philosopher (c. 470–399 BCE) considered one of the founders of Western philosophy.

Making a plan

Some things to consider

Strategic Oversight: You must be able to align with the board's strategic vision for the organisation. If you don't know what that vision is, ask them. They need to share their vision so you can plan effectively.

Risk Management: The board focuses on a risk-based view – and so must you. Use a common language and focus on how the plans you're making address the risks the boards face.

Reporting on Risk: Make sure any regular reporting to the board focuses on risks, how they have crystalised, new risks identified, and risks avoided.

Making a plan

Some things to consider

The Risk Landscape: The board needs to know that you are addressing risks from across the landscape. When you approach them with a request, put it in the overall context of all the risks.

Residual Risk: No matter how well you treat a risk, there will be some degree of risk that remains. Make sure this is clear to the board and that by accepting a certain option, they also accept the residual risks.

Questions?