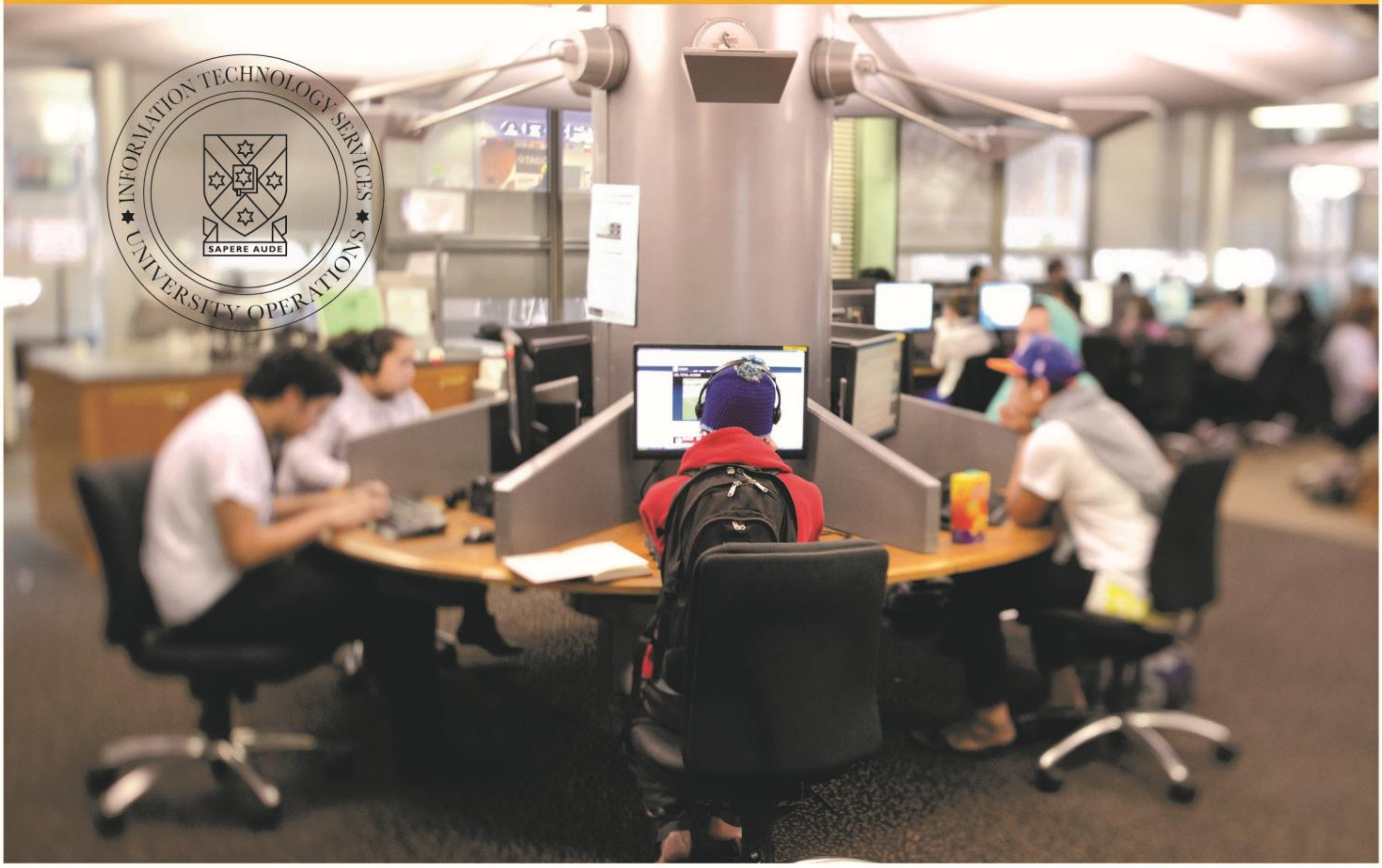


Cyber Security Framework

November 2022

Document Version 1.1

University Operations

Information Technology Services

Campus and Collegiate Life Services | Campus Development | Chief Operating Officer
Health and Safety Compliance | Project Management | Property Services
Risk, Assurance and Compliance | Shared Services | Sustainability

University of Otago | PO Box 56 | Dunedin 9054 | New Zealand

Enable | Engage | Experience

Acknowledgements

IT Assurance and Cyber Security acknowledge those who created the referenced materials below. These have created the foundation and context for this framework.

These resource documents have been relied on for development of this framework:

- 'Cyber Security Framework' – National Institute of Standards and Technology
- NIST 800 series documents - National Institute of Standards and Technology
- 'CIS Controls version 7' – Centre for Internet Security
- AS/NZS 27000 series of documents – ISO
- COBIT 2019 Framework documents – ISACA
- 'IT Risk Framework' – ISACA
- 'AS/NZS 31000:2009 Risk management – Principles and guidelines - ISO
- ISA 62443 - Security for Industrial Automation and Control Systems – ISA / IEC
- 'Enterprise Security Architecture – A Business Driven Approach' - CMP Books
- 'Risk Management Framework' – University of Otago
- 'Project Management Framework' - University of Otago
- Open-Source Security Testing Methodology Manual – ISECOM
- OWASP Project documentation

Intent

This Cyber Security Framework defines the structure and operation of the cyber security program across the University of Otago. It assures governance of cyber security across the University and provides a feedback loop for continuous improvement. There are underlying processes, standards, guides, checklists, etc., that further define and support the operation of this framework.

Use

IT Assurance and Cyber Security owns and operates the Cyber Security Framework on behalf of the University of Otago. All other individuals or groups are expected to support this team in implementing the framework and working towards achieving the goals and outcomes defined in this framework.

Change

Changes can be made with approval of Director ITS where there is no material impact or significant variation.

Version

Date	Version	Change	By
28 September 2018	0.1	Initial version	R. Feist
4 March 2019	0.3	Released for Peer Review	R. Feist
9 May 2019	0.5	Released for wider Peer Review	R. Feist
21 June 2019	0.7	Feedback incorporated	R. Feist
30 June 2019	0.8	Feedback Policy Management Group	R. Feist
25 July 2019	0.9	Feedback IT Governance Board	R. Feist
18 October 2019	1.0	Version 1	R. Feist
30 November 2022	1.1	Updated information security classification scheme to align with Information Management Framework and with the basic guidelines on handling of the classified information	Gareth Wood & Umair Zia

CONTENTS

INTRODUCTION

From the 'University of Otago - Strategic Direction to 2020' document:

Vision

"A research–led University with an international reputation for excellence"

Mission

"The University of Otago will advance, preserve, promote, and apply knowledge, critical thinking, and intellectual independence to enhance the understanding, development and well-being of individuals and society. It will achieve these goals by building on foundations of broad research and teaching capabilities, unique campus learning environments, its nationwide presence and mana, and international links."

With our increasing reliance on technology to manage information, the reliable functioning of the information technology (IT) infrastructure and the protection of our data is critical in supporting business decisions. The likelihood and potential impacts of an information security incident on the University, the health and safety of individuals, the environment, communities, and the broader economy and society is also increasing.

Information assets exist in many forms; printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on video, or spoken in conversation. Whatever form they take, or by which they are transferred or stored, their value should be understood and must be appropriately and consistently protected across all storage, processing, and exchanges.

Attacks on information systems and data are usually attempts to compromise the people, processes, or technology systems in some manner. The potential consequences of poor or inconsistent information security include:

- Unauthorised access (Confidentiality): An attacker might steal patient records, student records, research data or other unique information to impersonate someone, on-sell or otherwise cause damage to the University.
- Deletion or alteration of information (Integrity) - An attacker might delete or change the University's research data, records or deface its public web sites.
- Disruption of normal business operations (Availability): An attacker can launch a denial-of-service or ransomware attack, making it impossible for legitimate users to access the information systems in a timely manner.
- Damage to persons (Safety): Any of the above could result in risk to the personal safety of the University or 3rd party staff or students.

In recent times we have seen the traditional network perimeter 'dissolve' due to the rise of the mobile employee and the increasing adoption of cloud services. This 'traditional' approach to information security was policy heavy and often failed or hampered the organisation due to complexity and rigidity. We are having to adjust rapidly to a more contemporary approach that is more pragmatic and agile while enabling the University to achieve its goals by having strong capabilities and processes around monitoring activity around information and responding proactively to maintain the required level of information security while allowing for the interactions a modern organisation's business processes demand.

Goals

The intent of the Cyber Security Framework is to facilitate excellence in Cyber Security which in turn will 'enable' the University to achieve its goals while protecting its people, processes, technology systems and data assets.

The more specific goals for the Framework are to:

1. ensure investment in security is effective in terms of financial cost and resulting protection of assets.
2. ensure the people are enabled (e.g., trained) to protect the security of data and systems they use.
3. ensure the efforts of all IT disciplines and specialties are working to a common defined understanding of the security that results in ubiquitous, efficient, and effective security delivery.
4. facilitate informed executive decision making through comprehensive risk management that delivers in a timely manner.
5. identify where shared security services and reuse of security strategies and tools can reduce development cost and delivery while improving security posture.
6. ensure collaboration across various operational teams to develop and operate appropriate controls, tools, processes, and techniques to build security in.
7. ensure that mandatory security controls can be applied without compromising technical and business functionality.
8. provide early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation.
9. provide a consistent method for assessing the security risks associated with the University.
10. transform security needs into security policy, standards, processes, and technology solutions.
11. establish confidence or assurance in the correctness and effectiveness of security mechanisms.
12. ensure that operational impacts due to residual security vulnerabilities in systems are in an acceptable range and that systems and processes exist to mitigate these efficiently.

Benefits

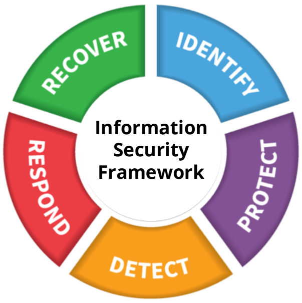
The benefits to the University of Otago of consistently managing cyber security across all areas include:

1. enabling the achievement of the organisation's mission through the consistent protection of confidentiality, integrity, availability and safety of information and people.
2. increasing resilience to Cyber Security attacks through improved controls, greater predictability, and reduced uncertainty.
3. enabling effective and timely response to evolving security threats.
4. managing the costs related to cyber security.
5. enhancing university culture in respect to information security at work and at home.
6. improving decision making through providing better information to support analysis, decision-making, and risk identification. Provide assurance that critical decisions are not based on faulty information.
7. improving compliance and reducing the related potential liability.
8. establishing accountability for safeguarding information through definition of clear roles and responsibilities that enable people to meet expectations.

CYBER SECURITY FRAMEWORK

The Cyber Security Framework defines how we implement, evaluate, and improve cyber security practices throughout the University of Otago. It allows us to articulate goals and drive ownership of them while also evaluating and improving cyber security over time. It is expected that the framework will develop over time as the organisation matures in respect to governance of information security.

The Cyber Security Framework is aligned with other University Frameworks including the Risk Management Framework, Information Management Framework and Project Management Framework.



Scope

To foster a 'whole of university' approach to cyber security to achieve our strategic objectives and ensure our valuable data assets are managed appropriately.

The scope of the Cyber Security Framework includes:

- All University owned data, hardware, software, and services regardless of location
- All University staff, contractors, guests, and students.

The daily management of the security of assets is delegated to appropriate groups who take on the responsibility for ensuring these are secured, e.g., server team looking after a web server.

Organisational Culture and Behaviour

The culture and behaviour toward Cyber Security within the University is crucial to achieving the goals and benefits. As Cyber Security is highly dependent on people it is important that there is visible senior management support, user education and that change is managed as a key part of the continual improvement cycle with particular focus on ensuring that resistance is addressed, and that the framework is applied ubiquitously.

The framework aims to build a culture of 'security and privacy by design'.

Framework Structure

The Framework provides:

1. a structured approach that at a high level is defined as set of activities and outcomes.
2. a way of describing our current Cyber Security posture.
3. a way of describing our target state for Cyber Security.
4. a mechanism for us to identify and prioritise opportunities for improvement within the context of a continuous and repeatable processes.
5. a mechanism for us to assess progress toward the target state.
6. a mechanism for communicating among internal and external stakeholders about Cyber Security risk.

The Framework is composed of groups of activities aimed at achieving specific Cyber Security outcomes and provides direction on how to achieve and measure those outcomes.

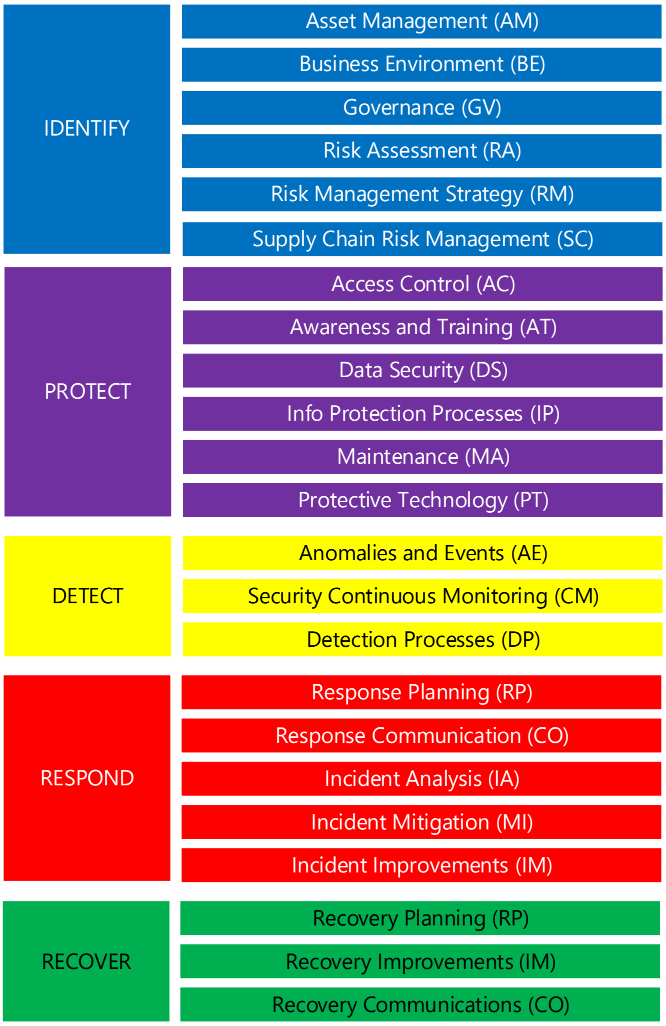
The Core elements work together as follows:

- The 5 Functions of Identify, Protect, Detect, Respond, and Recover group the Cyber Security activities at their highest level.
- Activities are groups of Cyber Security outcomes within each Function.
- Outcomes provide a set of results that support achieving each Activity.
- Standards define the expectations, as rules, that we establish regarding the configuration and operations of security to achieve the Outcomes. These may be due to government, or statutory requirements enforced by law, contractual obligations, or organisational choice to limit risk. An example of these are the rules relating to passwords or sharing of sensitive information.

Functions and Activities

The framework groups activities into the following 5 functions:

- IDENTIFY – Develop an organisational understanding to manage cyber security risk to systems, people, assets, data, and capabilities to enable the University to focus and prioritise its efforts, consistent with its risk management strategy and business needs.
- PROTECT – Develop and implement appropriate protection across people, process, and technology to prevent, limit or contain the impact of a potential cyber security event.
- DETECT – Develop and implement appropriate activities to proactively identify the occurrence of cyber security events.
- RESPOND – Develop and implement appropriate activities to take action regarding a detected cyber security incident. It also aims to limit or contain the impact of a potential cyber security incident.
- RECOVER – Develop and implement appropriate activities to maintain plans for resilience and to restore, in a timely manner, any capabilities or services that were impaired due to a cyber security incident.



IDENTIFY	Asset Management (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
	Risk Management Strategy (RM)
	Supply Chain Risk Management (SC)
PROTECT	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Info Protection Processes (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT	Anomalies and Events (AE)
	Security Continuous Monitoring (CM)
	Detection Processes (DP)
RESPOND	Response Planning (RP)
	Response Communication (CO)
	Incident Analysis (IA)
	Incident Mitigation (MI)
	Incident Improvements (IM)
RECOVER	Recovery Planning (RP)
	Recovery Improvements (IM)
	Recovery Communications (CO)

Figure 1 - Functions and related Activities

Further details of the Activities and their underlying Outcomes are given in Appendix A. These are directly taken from the industry standard NIST Cyber Security Framework and are specific to the cyber security context. They in turn link to further standards-based documentation that we will be using and as such should not be changed.

Policy

The Cyber Security Policy dictates that the Cyber Security Framework is implemented consistently and ubiquitously across the University.

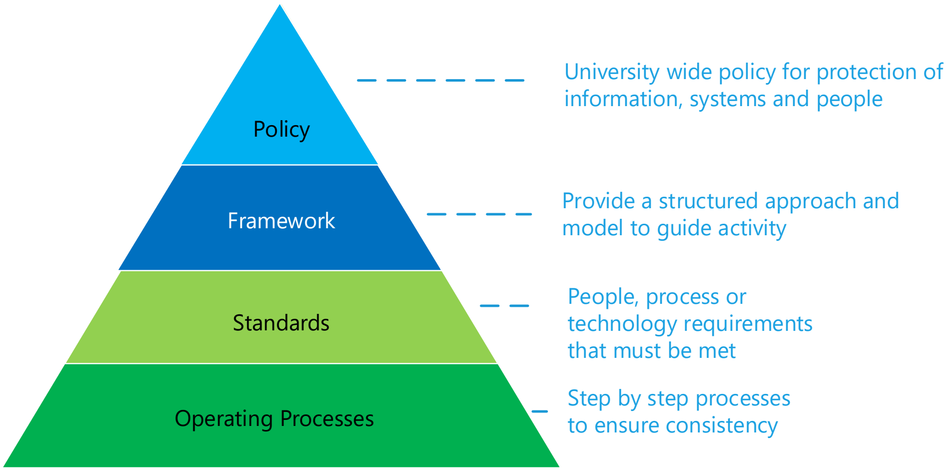

Policy
Framework
Standards
Operating Processes
University wide policy for protection of information, systems and people
Provide a structured approach and model to guide activity
People, process or technology requirements that must be met
Step by step processes to ensure consistency

Figure 2 – Cyber Security Framework and Policy structure

The Framework itself supports and assures the implementation of policy as a security control and provides feedback into policy for improvement.

Standards

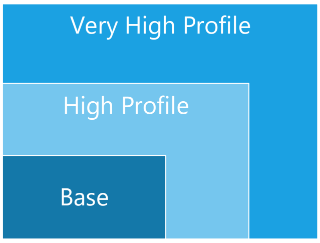
Standards are developed and maintained for each Activity. These must be applied consistently and ubiquitously across the University as per the Cyber Security Policy to gain the expected Outcomes and benefits.

The Standards are developed using the industry best practice Reference Standards (see Appendix A) as guidance while also accounting for the University's own requirements and risk appetite. They are more specific or detailed than policies and need to be easier to update in response to changing circumstances. The Standards set the minimum level of action needed to comply with a policy.

Within the Standards there is a subset that makes up a Base Security Profile. The Base Security Profile must be applied appropriately to everything as a minimum. Where a system or service requires a higher level of security then the Base Security Profile is augmented with additional standards. The assessment of the level of required security level is based on a risk assessment.

Security Profiles

The Base Security Profile consists of a set of common controls we need to run across the whole University due to the inherent risk in the operating environment and with the aim of reducing risk to an acceptable level. These profiles are made up of controls that span all the activities in the framework.



When the assets we need to protect have higher risk levels due to a specific set of data e.g., patient information or credit card details, it is often more practical and cost effective to apply controls at a system or service level. For example, all Finance 1 servers, or the payment Card Data Environment (CDE).

Additional High and Very High Security Profiles can be used as required to enhance or raise the level of protection over the Base Security Profile. Further Profiles may be developed over time to suit requirements.

By assessing the risk and classifying assets based on their inherent risk we are able to understand where we need to apply a higher level of security controls. Security Classification allows us to do this in a manner consistent with the risk model and to use this when defining what security controls are required to protect assets.

These Profiles are elements of the Standards that define the controls.

The Standards are supported by Processes and Guides where:

- Processes are often step-by-step instructions that are particular to a task, technology, or department. They are updated in response to changing technical or business influences. They can also provide a checklist to ensure consistency.
- Guides specify recommended actions and advice. Staff, students and third parties may not be required to follow guides as part of their jobs, but the guides are shared in order to promote good Cyber Security practices.

Cyber Security Management

Cyber Security management defines how the framework is put into practice. To achieve a holistic management of security we split Cyber Security Management into the following four high level processes:

- Security Engineering - engineering disciplines work together to develop and implement and operate secure systems or services for the organisation.
- Risk Management - identifies and prioritises vulnerabilities or weaknesses in proposed or implemented systems or services.
- Security Operations – all monitoring, identification, prevention and response activity.
- Assurance – all overarching activity to provide assurance that framework, processes and underlying security controls are delivering an effective level of security.

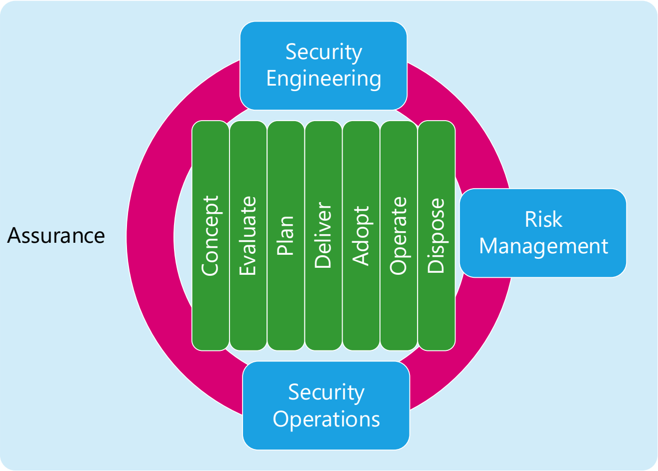


Figure 3 – High Level Security Management Processes

These processes are carried out across the Information Systems Development Life Cycle (SDLC)[1]. , from Concept to Disposal, of a system or service. They work in concert to ensure security controls are adequate and effective and that the intended protections are achieved.

The Concept to Adopt stages are aligned with the PMO's 3PM methodology. The Operate and Dispose are typically operational activities.

Further detail of these processes is documented in:

- 'Cyber Security Framework – Security Engineering Process'
- 'Cyber Security Framework – Risk Management Process'
- 'Cyber Security Framework – Security Operations Process'
- 'Cyber Security Framework – Assurance Process'

Security Engineering Process

Security Engineering, like other engineering disciplines, is a process that proceeds through the stages of the SDLC. Throughout this process, security engineers must work closely with the other parts of the greater engineering and operations teams within and outside of Information Technology Services (ITS) to mitigate security risk. To this end, security must be an integral part of the larger processes, and not a separate and distinct activity. It ultimately must result in 'security by design'.

Specific security deliverables are developed in the SDLC to ensure a consistent and reliable delivery. These will be detailed in the 'Cyber Security Framework – Security Engineering Process' document and will be integrate with the ITS 3PM and Change Management processes.

The process follows a security architecture driven approach to provide a consistent, comprehensive, top-down, end-to-end handling of security and can be applied to network elements, services, applications, and data in order to prevent, detect, predict, and correct security vulnerabilities or weaknesses. It also addresses the minimum-security requirements that include compliance, privacy, etc.

The process must produce adequate Requirements, Design, Implementation and Change Management documentation that is required during both Risk Management and Assurance process activity carried out as part of the SDLC and to support compliance claims when audited.

Further documents supporting the Framework will provide additional guidance to the engineering process the enable it.

Risk Management Process

Risk is defined as the "effect of uncertainty on objectives" in ISO 31000[2]. In Cyber Security terms we look at the objective, e.g., maintaining the confidentiality of student or medical records, and then examine the threats that may cause the risk to eventuate and try and place controls to effectively mitigate these.

Due to the complex, interconnected nature of the IT environment, we need to consider risks individually to ensure appropriate controls are used and in combination to ensure that weaknesses in one area don't expose another area. This is also a crucial part of ensuring that the overall financial spend on security controls is effective.

[1] Adapted from NIST SP 800-64 Security Considerations in the Information System Development Life Cycle to match the Project Management Framework

[2] ISO 31000 :2018 Risk management -- Guidelines

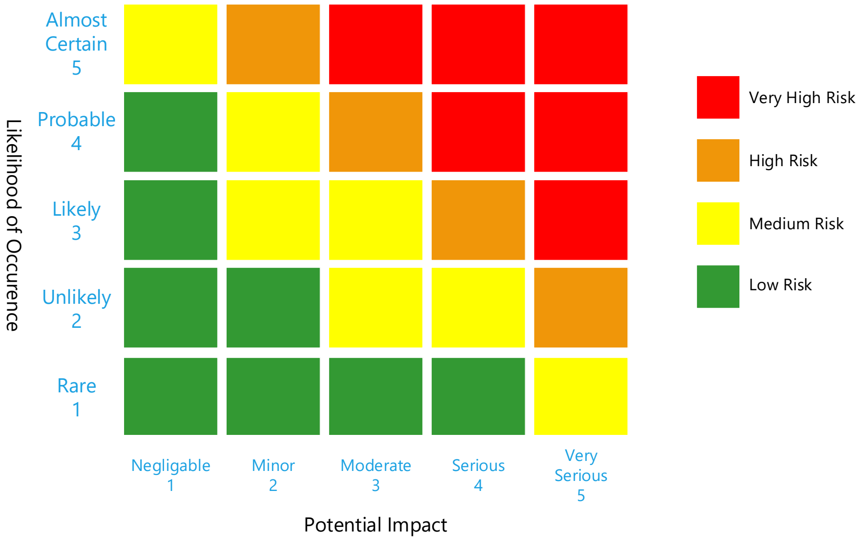
To address risk, additional tools and techniques are introduced to help identify and handle risks in the Cyber Security domain. These will be detailed in the 'Cyber Security Framework – Risk Management Process' document.

The Cyber Security Risk Management Process defines how risk is assessed in a cyber security context at key points in the SDLC to ensure risk treatment decisions are made with the appropriate considerations.

The Framework uses the following four risk categories to identify and understand Cyber Security risks to an asset (something of value):

- Confidentiality (includes Privacy) – ensuring information is not made available or disclosed to unauthorised individuals, entities, or processes.
- Integrity – ensuring that information cannot be modified in an unauthorised or undetected manner.
- Availability - ensuring that information is available when it is needed.
- Safety – ensuring that we understand when a failing in Confidentiality, Integrity or Availability can impact people safety.

Risks are categorised as per the University's Risk Management Framework criteria and matrix.



	Negligable 1	Minor 2	Moderate 3	Serious 4	Very Serious 5
Almost Certain 5	🟨	🟧	🟥	🟥	🟥
Probable 4	🟩	🟨	🟧	🟥	🟥
Likely 3	🟩	🟨	🟨	🟧	🟥
Unlikely 2	🟩	🟩	🟨	🟨	🟧
Rare 1	🟩	🟩	🟩	🟩	🟨

🟥	Very High Risk
🟧	High Risk
🟨	Medium Risk
🟩	Low Risk

Figure 4 - Risk Matrix as per University's Risk Management Framework

Exceptions

Exceptions are handled on a case-by-case basis and require a risk assessment. Based on the outcome of this, an exception may be granted for a period of time, will require a plan to correct and be handled as a risk. In some cases, exceptions may require compensating controls to manage the risk they present to the wider University.

Security Classification of Information

Information needs to be considered and handled as an asset. To assist with protection of this type of asset we need a model for assigning a security classification in a consistent manner. Once a classification is assigned then this informs users of the type of handling that is required for the Asset to ensure its ongoing protection.

The security classification is an element of a much larger group of meta-data related to information assets.

The ‘matrix for security classification of information’ would be used to allow a consistent assessment of the risk attributed to sets of information or a system that holds the information, e.g student information or payment card data, to inform the requirements and design process so that the appropriate level of controls are applied.

The following matrix for the security classification of information applies:

INFORMATION SECURITY CLASSIFICATION		BASIC GUIDELINES ON HANDLING OF THE CLASSIFIED INFORMATION			
Label	Description	Information Sharing	Transmission	Storage *Must comply Information and Rec Management Stan under the Public Rec Act 2005) * As per Mandatory Solutions and Services Data Storage Locations Guidance.	Disposal Method * Must comply Information and Rec Management Stan under the Public Record 2005)
PUBLIC Public Release Authorized	Information specifically created for public publishing or public disclosure authorised by appropriate University authority.	Information can be shared using approved University systems and services that have been established for publishing to public.	Electronic Transmission: • Information can be transferred using approved University systems and services for Public information.	Information is subject to University requirements.	Information is subject to University requirements.
INTERNAL USE Access Limited to Internal Use Only	Disclosure of this information to an unauthorised party is not likely to adversely affect the University or the privacy of any individual. Information about University operations not intended for an external audience and not containing sensitive business information or non-public personal information	Information can be shared internally and with others with a formal relationship with the University (e.g., contracted vendors) as appropriate to circumstances and where relevant to their role or function (there is a 'need to know'). Only via approved platforms or services that implement appropriate controls	Electronic Transmission: • Information can be transferred using approved University systems and services. Paper Transmission: • Sealed envelope stating recipient and postal address e.g., internal mailbox number.	Electronic and paper-based information must be stored in a manner that has protections against unauthorised access, theft, vandalism, or misuse.	Electronic Disposal: • Electronic files, magnetic and other storage media must be disposed of in a way that makes compromise highly unlikely. • Magnetic and other storage media should be sanitised in manner that makes reconstruction highly unlikely (DOD 5220.22-M)

					• Magnetic waste e.g. CDs, tapes, videos **should be** securely disposed of using secure destruction services. Paper Waste Disposal: • Disposed of as per Universities Records Destruction Guidelines.
CONFIDENTIAL Access Limited to Authorized Personnel	Disclosure of this information to an unauthorised party would adversely affect the University or the privacy of any individual. Information about any identifiable individuals (personal Information) and strategic or commercial business information. Any information that has been provided in confidence, or where there are contractual requirements for confidentiality.	Information may not be shared except with appropriate authorisation. Personal information is subject to the Privacy Act 2020 and the Policy on Access to, and Use of, Personal Information. CONFIDENTIAL information may be shared via approved platforms or services that implement appropriate controls Should have a non-disclosure agreement or contract/authorisation in place prior to sharing outside of University. Where information is to be sent outside of New Zealand, the requirements set out in the Privacy at Otago webpage have been	Electronic Transmission: • Username/password access control should be considered • Encrypted transmission should be considered • Labelling documents CONFIDENTIAL is recommended where practical. • Adding CONFIDENTIAL at start of Subject for email • An appropriate statement should accompany all CONFIDENTIAL information transmitted via email Paper Transmission • Documents **must** be posted in a sealed envelope and labelled CONFIDENTIAL and have a return address. • **Must be** sent via recognised postal services or commercial courier firms.	Electronic and paper-based information must be stored in a manner that has protections against unauthorised access, theft, vandalism, or misuse. Access should be limited to people with a normal business need to access the information. This should be built into IT systems or physical access controls where possible. Electronic Storage: • University systems should only use the centralised authentication service to manage access • At minimum the storage systems should require authentication (or	Electronic Disposal: • Electronic files, magnetic and other storage media **must** be disposed of in a way that makes compromise highly unlikely. • Magnetic and other storage media **must be** sanitised in manner that makes reconstruction highly unlikely (DOD 5220.22-M) • Magnetic waste e.g. CDs, tapes, videos **must be** securely disposed of using secure destruction services. Paper Waste Disposal • Disposed of as per Universities Records Destruction Guidelines.

		met (Information Privacy Principle 12).		decryption key) to access data. Paper Storage: • Physical information should be in a secure environment, with offices locked when unattended and unsupervised, and information not visible to visitors. • Physical information taken off-site must be kept secure and should be additionally protected from theft (e.g., locked drawer or cabinet)	
RESTRICTED Access Limited to Authorized Personnel	**Disclosure of this information to an unauthorised party would be likely to seriously damage the University or endanger the safety of any individual.** Very sensitive personal information (includes health information or about sensitive matters) Sensitive strategic or commercial business information	Access to RESTRICTED information must be limited to individuals authorised by the information owner RESTRICTED Information may only be shared with the authorised individuals Personal information is subject to the Privacy Act 2020 and the Policy on Access to, and Use of, Personal Information. RESTRICTED information must only be shared using approved platforms or services that implement appropriate controls	Electronic Transmission: • Username/password access control and/or encryption is required • Information must be encrypted when transmitted • Labelling documents RESTRICTED is recommended where practical. • Adding RESTRICTED at start of Subject for email • An appropriate statement should accompany all RESTRICTED information transmitted via email Paper Transmission:	Electronic and paper-based information must be stored in a manner that has protections against unauthorised access, theft, vandalism, or misuse. Access should be limited to people with a normal business need to access the information. This should be built into IT systems or physical access controls where possible. Electronic Storage: • Electronic files must be protected against	Electronic Disposal: • Electronic files, magnetic and other storage media must be disposed of in a way that makes compromise highly unlikely. • Magnetic and other storage media must be sanitised in manner that makes reconstruction highly unlikely (DOD 5220.22-M) • Magnetic waste e.g. CDs, tapes, videos must be securely disposed of using

	Seriously damage the interest of Otago if prematurely disclosing information relating to decisions, trade secrets, agreements, or commercials activities. Any information that has been provided in confidence, or where there are contractual requirements for limited access	Requires that a non-disclosure agreement or contract/authorisation is in place prior to sharing outside on University. Where information is to be sent outside of New Zealand, the requirements set out in the Privacy at Otago webpage have been met (Information Privacy Principle 12).	• Documents must be posted in a sealed envelope and labelled RESTRICTED for addressee only and have a return address. • Must be sent via recognised postal services or commercial courier firms. • The use of double envelopes may be considered.	inappropriate use or unauthorised access. • Risk mitigation controls must be appropriate and in accordance with the University's Risk Management Framework and the Cyber Security Framework. Paper Storage: • RESTRICTED documents must be protected against unauthorised access by storing them separately from other files, and in locked drawers or cabinets. The storage areas should be intruder resistant with security measures applied e.g. building security, door swipe system.	secure destruction services. Paper Waste Disposal • Disposed of as per Universities Records Destruction Guidelines.

Figure 5 - Matrix for Security Classification of Information

The criteria for assessing the level of risk, the threats and the effectiveness of controls change over time. The risk assessment allows for this and there is regular review of the assessed risks, threat and effectiveness of controls.

To address security classification, we are introducing additional tools and techniques to help identify and handle security classification in the Cyber Security domain. These will be detailed in the 'Cyber Security Framework – Security Classification of Information Process' document.

Assessing Risk and Control requirements

Security controls are applied to reduce risk and mitigate threats to assets (e.g. data, processes, systems or people). When assessing risk, we need to understand likelihood and impact but also temper this with reality. In this context, we need to account for the fact that it is frequently the low-risk systems that are initially compromised in high impact events and that we are dealing with frequent targeted attacks. The Base Security Profile is an important in this respect.

Likelihood

In the Cyber Security field, we start with a default assessment of likelihood as:

Criteria	Likelihood	
Systems/service/asset is visible or accessible from off-campus	Probable	The Internet is a hostile environment, and we continually see active probing or attacks.
Systems/services only accessible from on campus or via approved VPN	Likely	The internal network can be more secure but we still have a large volume of uncontrolled systems e.g. BYOD, students on the network.

Impact

The impact is dependent on the type and value of asset, its use within the organisation and the nature of the threat. The Risk Management Framework provides a set of assessment criteria that can be used to determine the level of Impact.

Inherent Risk

This is derived by assessing the risk without controls and is calculated as Likelihood x Impact = Inherent Risk.

Risk Ownership

To ensure that all information assets receive the appropriate level of protection each should have an information custodian who is the de-facto 'risk owner'[3] responsible for the information including ensuring that appropriate cyber security controls are in place.

Applying Controls

To address/mitigate the Inherent Risk we need to apply controls. Due to the nature of digital information, this is relatively complex, especially when applying the principles of 'defence in depth' and 'Security by Design'. To simplify this process, we define sets of controls as Profiles and apply the Base Security Profile as a minimum.

[3] Risk owner as defined in the Risk Management Framework

We need to ensure that we manage the financial cost vs benefits to ensure that we are cost effective in terms of the application of the controls.

Staff managing the information assets on behalf of the information custodians are expected to apply, operate, and monitor appropriate controls while custodians are expected to ensure these controls are applied and are functioning correctly.

Security Operations Process

Security Operations is the specific activity carried out by IT Assurance and Cyber Security in collaboration with ITS operational teams and departments to ensure that the systems and services are safe and secure. This entails operating security services that include:

- Authentication, Authorisation and Accounting (AAA) – Monitoring of authentication and authorization to resources, identifying abnormal behaviour and alerting on this
- Cyber Security Awareness Education – key element for improving customer awareness of their role in Cyber Security, ensuring they are able to meet their obligations under Policy. For specialist roles with Cyber Security responsibilities, there is additional role specific training.
- Vulnerability Assessment (VA) – scans the external and internal network on a scheduled basis, identifies devices on the network and the services they run, and then examines these for known vulnerabilities or weaknesses. Reports this as metrics and is used to identify risk and trigger remediation activity.
- Intrusion Detection System (IDS) – monitors network traffic and behaviour for known bad patterns and/or content and automatically blocks, alerts, or triggers incident response activity.
- Security Information and Event Management (SIEM) – receives data from sensors, other security services and system alerts. Enables operators to investigate and action. Key element/tool in Incident Response
- Endpoint Protection (EP) – new generation of Antivirus to protect devices, reports metrics and triggers remediation activity. May block, quarantine, or alert. This is able to monitor devices on-premises and remotely where they have internet access.
- Threat Intelligence – security information feeds from various external sources that are used by SIEM or operators to identify bad activity. These also provide contextual awareness.
- Infrastructure firewalls - Firewalls are used to allow only approved network traffic. Filtering can be done on basic source / destination and via deeper inspection of the traffic to identify and prevent known bad or malicious content. Includes inspecting within encrypted content e.g., SSL Inspection.
- Web Application Firewalls – monitor content being exchanged with web services and used to identify and block command injection or other types of web application attacks.
- Cyber Security Incident Response – Process and tools to facilitate speedy handling and return to service. This is highly dependent on the other security services for limiting impact and effective response.
- Security Risk and Compliance – Platform to managed Cyber Security risks, activities, and reporting. Also called a Governance, Risk and Compliance (GRC) system.
- Cyber Security Dashboard – Real time reporting.

Assurance Process

This is the overarching activity to provide assurance that Framework, processes, and underlying security controls are delivering an effective level of security and the reporting of this at both the management and governance levels.

Reporting will be provided as:

1. Near Real-time Dashboards based on activity

2. Monthly reporting within ITS
3. Quarterly reporting to Audit Risk and Compliance, VCAG and other senior management as required.

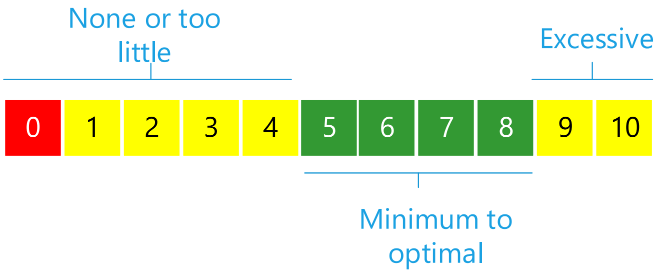
The assurance process also directs continuous improvement of the Framework, processes, and the underlying controls.

This will be detailed in the 'Cyber Security Framework – Assurance Process' document.

Framework Assurance

Assurance that the Cyber Security Framework is operating at an acceptable level is provided by the reporting of the Framework state using the following measurement process.

The Framework is measured on the following scale:



Score	Matching Criteria
0	Cannot determine if outcome has ever occurred.
1	Outcome rarely/never happens when needed.
2	Outcome happens unreliably when needed. Errors, flaws and re-work common.
3	Outcome happens unreliably when needed. Re-work is common.
4	Outcome happens consistently with error, flaws and some rework.
5	Outcome happens consistently with some error, occasional flaws.
6	Outcome happens consistently, but not as effectively as required or quality is lower than required.
7	Outcome happens consistently.
8	Outcome happens consistently with great effectiveness and high quality.
9	Outcome happens at higher financial cost while meeting the requirements with limited additional benefit to the University.
10	Outcome happens at excessive financial cost or exceeds the requirements with no tangible benefit to the University.
N/A	Not Applicable.

Figure 6 - Scale Criteria

Target Score

A target score is set for each Activity that is representative of the risk and level of protection that is required. This is reviewed quarterly as part of the reporting preparation.

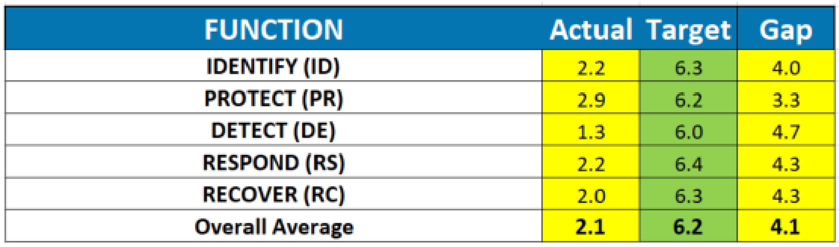
During assessment the mean average of the outcomes related to the Function and Activities is used to compare the assessed state to the target. The gap is the difference between target and actual scores and is used to identify areas that need deeper investigation or improvement.

Cyber Security Scorecard

A Cyber Security Scorecard will be maintained and reported quarterly. This will provide a view of the state of Cyber Security for the University of Otago. This will:

1. Identify the overall state of Cyber Security Framework in respect to governance targets.
2. Identify the top risk areas as per the Framework activity.
3. Show overall view of Framework state.
4. Show projects / work in progress to reduce / mitigate risk.

Examples of elements in the scorecard include:



FUNCTION	Actual	Target	Gap
IDENTIFY (ID)	2.2	6.3	4.0
PROTECT (PR)	2.9	6.2	3.3
DETECT (DE)	1.3	6.0	4.7
RESPOND (RS)	2.2	6.4	4.3
RECOVER (RC)	2.0	6.3	4.3
Overall Average	**2.1**	**6.2**	**4.1**

Figure 7 - Example of Overall state of the Cyber Security Framework

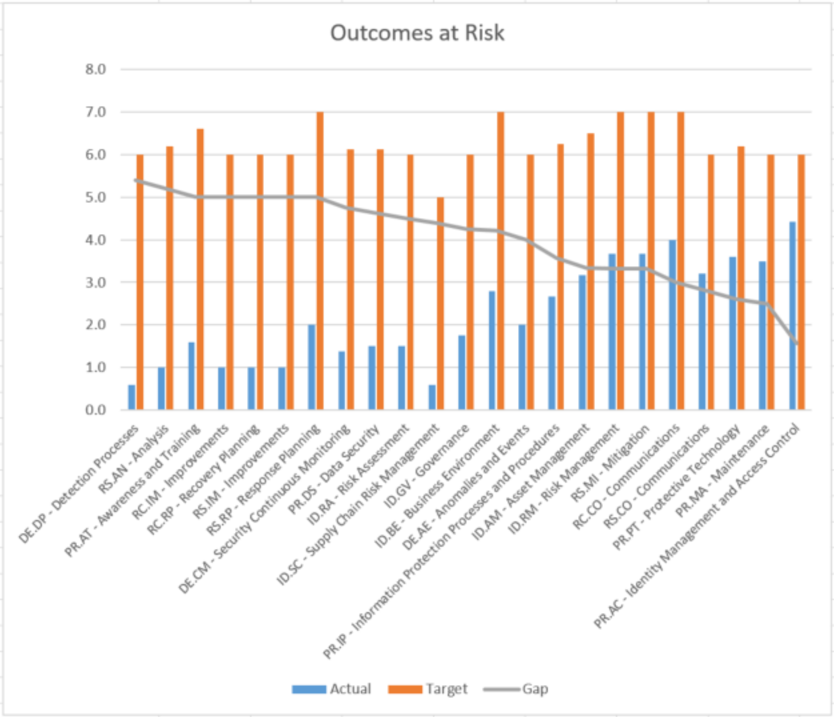


Figure 8 - Example of Activities at Risk (Gap)

This graph provides a view of the target value, the actual (currently assessed) value and the difference as the gap. This size of gap is an indication of potentially higher risk or need for attention. In this case, the item toward the left requires more action.

Security Management Reporting

Reporting will be provided from the four security management processes to provide assurance on the effectiveness of security controls. This will be presented as:

Dashboards

- Near real-time operational metrics on one or more dashboards.

Monthly Report to Director ITS

- Security Engineering
  - Projects
  - Change Control
- Risk Management
  - Material changes in risk, including exceptions
- Security Operations
  - Operational security metrics from controls e.g., firewall, anti-virus, Office 365
  - Incident metrics

Quarterly Report to Audit Risk and Compliance, VCAG and senior management as required.

- Framework state
- Security Engineering
  - Projects
  - Change Control
- Risk Management
  - Risk register progress
  - Material changes in risk, including exceptions
- Security Operations
  - Operational security metrics from controls e.g., firewall, anti-virus, Office 365
  - Incident metrics

GOVERNANCE

Organisational Governance

Corporate Governance is the ‘ongoing activity of maintaining a sound system of internal control by which the directors and officers of an organisation ensure that effective management systems, including financial monitoring and control systems, have been put in place to protect assets, earning capacity and the reputation of the organisation’ (TSO, 2009).

In the context of Information Security, governance is achieved through a combination of governance and management activity as described below.

Information Security Governance

Information Security Governance ensures that:

- Stakeholder security needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives.
- Direction is set through prioritisation and decision-making.
- Risk and opportunity are balanced and fit with the organisation’s objectives.
- Performance and compliance are monitored against agreed-on direction and objectives.
- Appropriate governance level reporting is provided.

Information Security Governance is the responsibility of the governance and executive management of the University. This is denoted in the top layers of the Information Security Governance and Management Layers diagram above.

The IT Assurance and Cyber Security team performs the subset of cyber security activities on behalf of the higher governance levels and working with peers at the Portfolio Governance level and management below to ensure the goals are achieved.

Cyber Security Policy

The top-level Cyber Security Policy addresses the purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities to manage protection of information systems and assets within the scope of cyber security. This establishes the importance of, and expectations for, governance of cyber security across the University.

It provides the mandate for Cyber Security Management and the ubiquitous application of its controls, processes and standards across all people, IT infrastructure, devices and services used by the University in its operations.

Cyber Security Management

Cyber Security Management plans, builds, operates, monitors and reports on cyber security activities and controls, in alignment with the direction set by cyber security governance, to help achieve the University’s objectives. IT Assurance and Cyber Security performs the management function and combines with various ITS and other operational teams to perform the operational work to achieve this.

Information and Communications Technology Regulations 2014

The Information and Communications Technology (ICT) Regulations 2014 provides direction on use of University ICT.

IT Acceptable Use Policy

The IT Acceptable Use Policy provides direction on the basic responsibilities of all students, staff and contractors in respect to the protection of University data and systems and services they use or are responsible for.

These establish and communicate the behaviour that all users of information technology are required to practice to ensure protection of information assets, systems, and services.

General Roles and Responsibilities

The following section describes at a high level how the different groups and individuals play a part in cyber security.

Organisational Governance – Audit and Risk Committee and University Council

The Audit and Risk Committee is a Committee of the University Council. Its role is to strengthen the University's control environment and management of risks and to assist Council to discharge its leadership and control responsibilities for financial reporting and risk management.

IT Assurance and Cyber Security provide reporting from the Framework and on related cyber security risks as an input to the Audit and Risk Committee.

Executive Management

IT Assurance and Cyber Security provide reporting on the operations of the Framework and related cyber security service metrics and risks to the University's Executive Management via the Director ITS on a monthly basis and they in turn provide direction to the IT Assurance and Cyber Security based on this reporting.

Specialist Governance – IT Governance Board

The IT Governance Board provides high-level governance and oversight of IT activities at the University with the aim of ensuring that IT activities are successful in supporting the strategy and goals of the University. The IT Governance Board will also have oversight of the benefits realisation associated with IT investment. The IT parts of cyber security fall under their remit but this needs to be done in coordination with other governance bodies e.g., Audit and Risk Committee.

Specialist Management

IT Assurance and Cyber Security retains overall responsibility for defining, operating and reporting on Cyber Security and works with all other parties to ensure appropriate levels of security are applied. Where individual or group responsibilities intersect with cyber security a joint approach needs to be agreed. In the absence of this then the standard approach should be enforced to ensure a consistent level of security.

IT Assurance and Cyber Security reports on the operation of the framework to the Director ITS on a monthly basis and Director ITS in turn provides direction to IT Assurance and Cyber Security based on this.

IT Assurance and Cyber Security reports on the operation of the framework to the Audit and Risk Committee on a quarterly basis and they in turn provide direction to IT Assurance and Cyber Security based on this.

Other Individuals or groups within this Specialist Management level have specific areas of responsibilities across the University, and where appropriate or required interact with IT Assurance and Cyber Security to ensure cyber security is consistently managed.

IT Enterprise Architecture

IT Enterprise Architecture provides direction and guidance on the overall architecture, principles, standards, etc, for IT in the University. IT Assurance and Cyber Security works in collaboration with Enterprise Architecture to develop the security architecture for the University's IT systems.

Divisional Management – Directors, PVCs and DVCs

These actively ensure that their organisation is operating within the Cyber Security Policy and are expected to manage risk within their portion of the organisation. They are supported and advised by IT Assurance and Cyber Security.

Operational Management – Departments, Faculties, Schools or Units

These actively ensure that they are operating within the Cyber Security Framework and work with IT Assurance and Cyber Security to achieve this.

Individuals - Professional Staff, Academic Staff, Students and third parties

All staff and students are responsible for using services delivered under this framework in an acceptable manner. These conditions of use are detailed in the 'Information and Communications Technology Regulations 2014', 'Cyber Security Policy' and 'IT Acceptable Use Policy'.

Individuals – IT Staff and third parties

Staff with any IT administrative, application development or support responsibilities, irrespective of department, have greater responsibilities and must work as per the underlying cyber security standards, processes, guides, and playbooks. These staff play a key part in the overall security of the University IT environment due to their level of access and control over University IT systems or services.

Security Awareness Education will also include information to ensure individuals understand and are able to meet their specific responsibilities.

Stakeholder Relationships

The following diagram describes the stakeholder relationships for cyber security. All stakeholders have a

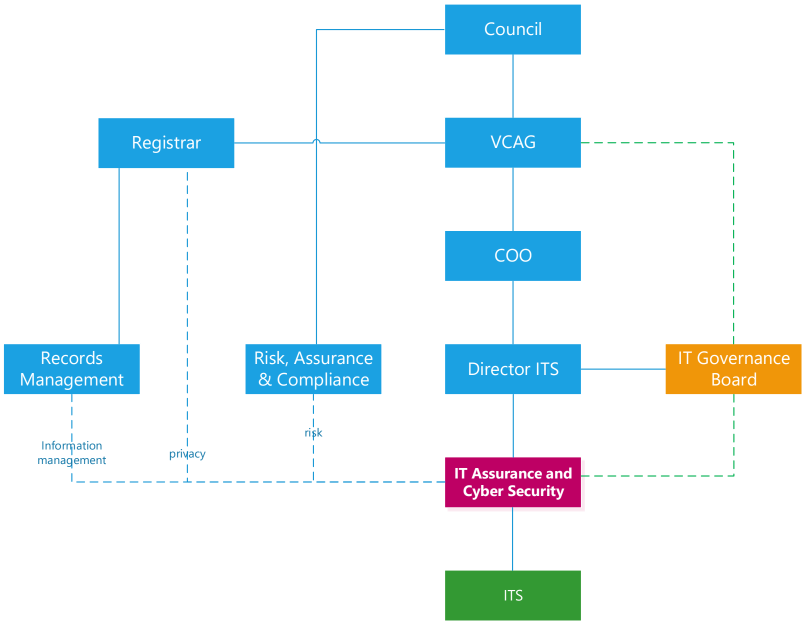


Figure 9 - Information Security Stakeholder Relationships

APPENDIX A – FRAMEWORK

This table describes the core elements of the Cyber Security Framework.

NOTE: We need to incorporate NZ Information Security Manual, NZ Protective Security Requirements and NZ Health Information Security Framework that are potential compliance requirements.

Activity	Description	Outcome	Reference Standard/s
Asset Management (ID.AM)	The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy.	ID.AM-1: Physical devices and systems within the organisation are inventoried.	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organisation are inventoried.	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organisational communication and data flows are mapped.	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued.	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritised based on their classification, criticality, and business value.	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6

		ID.AM-6: Information security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
Business Environment (ID.BE)	The organisation's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform information security roles, responsibilities, and risk management decisions.	ID.BE-1: The organisation's role in the supply chain is identified and communicated.	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: The organisation's place in critical infrastructure and its industry sector is identified and communicated.	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organisational mission, objectives, and activities are established and communicated.	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14
Governance (ID.GV)	The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of information security risk.	ID.GV-1: Organisational information security policy is established and communicated.	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all security control families
		ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2

		ID.GV-3: Legal and regulatory requirements regarding information security, including privacy and civil liberties obligations, are understood and managed.	CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address information security risks.	COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
Risk Assessment (ID.RA)	The organisation understands the information security risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented.	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Information threat intelligence is received from information sharing forums and sources.	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented.	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified.	CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11

		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritised.	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9
Risk Management Strategy (ID.RM)	The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organisational stakeholders.	CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: Organisational risk tolerance is determined and clearly expressed.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: The organisation's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.	COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11
Supply Chain Risk Management (ID.SC)	The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has established and	ID.SC-1: Information supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders.	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9

	implemented the processes to identify, assess and manage supply chain risks.	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritised, and assessed using a Information supply chain risk assessment process.	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation's information security program and Information Supply Chain Risk Management Plan.	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Identity Management, Authentication and Access Control (PR.AC)	Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users, and processes.	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected.	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed.	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties.	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24

		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		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, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organisational 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
Awareness and Training (PR.AT)	The organisation's personnel and partners are provided information security awareness education and are trained to perform their information security related duties and	PR.AT-1: All users are informed and trained.	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13

	responsibilities consistent with related policies, procedures, and agreements.	PR.AT-2: Privileged users understand their roles and responsibilities.	CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities.	CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand their roles and responsibilities.	CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
Data Security (PR.DS)	Information assets are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected.	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected.	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained.	CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented.	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment.	CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.4.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7

Information Protection Processes and Procedures (PR.IP)	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).	CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented.	CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place.	CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested.	CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

		PR.IP-5: Policy and regulations regarding the physical operating environment for organisational assets are met.	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy or legislation.	COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6 NZ Public Records Act - GDA
		PR.IP-7: Protection processes are improved.	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 ISO/IEC 27001:2013 A.16.1.6, Clause 9, Clause 10 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared.	COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	CIS CSC 19 COBIT 5 APO12.06, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested.	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14

		PR.IP-11: Information security is included in human resources practices (e.g., deprovisioning, personnel screening).	CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: A vulnerability management plan is developed and implemented.	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
Maintenance (PR.MA)	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools.	COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 ·NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access.	CIS CSC 3, 5 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
Protective Technology (PR.PT)	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family

		PR.PT-2: Removable media is protected, and its use restricted according to policy.	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 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, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7
		PR.PT-4: Communications and control networks are protected.	CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Anomalies and Events (DE.AE)	Anomalous activity is detected, and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analysed to understand attack targets and methods.	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined.	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established.	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
Security Continuous Monitoring (DE.CM)	The information system and assets are monitored to identify information security events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential information security events.	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential information security events.	COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20

		DE.CM-3: Personnel activity is monitored to detect potential information security events.	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected.	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
		DE.CM-5: Unauthorised mobile code is detected.	CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential information security events.	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorised personnel, connections, devices, and software is performed.	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed.	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5
Detection Processes (DE.DP)	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

		DE.DP-2: Detection activities comply with all applicable requirements.	COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested.	COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated.	CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved.	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
Response Planning (RS.RP)	Response processes and procedures are executed and maintained, to ensure response to detected information security incidents.	RS.RP-1: Response plan is executed during or after an incident.	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
Communications (RS.CO)	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-1: Personnel know their roles and order of operations when a response is needed.	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8

		RS.CO-2: Incidents are reported consistent with established criteria.	CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans.	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader information security situational awareness.	CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15
Analysis (RS.AN)	Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated.	CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood.	COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4

		RS.AN-3: Forensics are performed.	COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Incidents are categorised consistent with response plans.	CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyse, and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g., internal testing, security bulletins, or security researchers.	CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15
Mitigation (RS.MI)	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained.	CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Incidents are mitigated.	CIS CSC 4, 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
Improvements (RS.IM)	Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned.	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

		RS.IM-2: Response strategies are updated.	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
Recovery Planning (RC.RP)	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by information security incidents.	RC.RP-1: Recovery plan is executed during or after an information security incident.	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
Improvements (RC.IM)	Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated.	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
Communications (RC.CO)	Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-1: Public relations are managed.	COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident.	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4

APPENDIX B - GLOSSARY

Assurance	All the systematic actions necessary to provide confidence that the target (system, process, organisation, programme, project, outcome, benefit, capability, product output, deliverable) is appropriate.
Best Practice	A defined and proven method of managing events effectively.
CARTA	Gartner's strategic approach for information security -- Continuous Adaptive Risk and Trust Assessment. Released 2018.
CAUDIT	Council of Australasian University Directors of Information Technology. We are members.
CIS CSC	Centre for Internet Security Critical Security Controls, is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organisations against cyber threats.
CMMI	Capability Maturity Model Integration, a process level improvement training and appraisal program developed at Carnegie Mellon University (CMU).
COBIT	Control Objectives for Information and Related Technologies is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance.
CSF	National Institute of Standards and Technology Cyber Security Framework.
EDUCAUSE	Global non-profit association and the largest community of technology, academic, industry, and campus leaders advancing higher education through the use of IT.
Issue	A relevant event that has happened, was not planned, and requires management action. Could be a problem, query, concern, change request or risk that has occurred.
ICT	Information and Communication Technology, often referred to as Information Technology (IT).
IDP	Intrusion Detection and Prevention.
IEC	International Electrotechnical Commission, an organisation that publishes international standards.
ISACA	Global a non-profit, independent association that advocates for professionals involved in information security, assurance, risk management and governance.
ISECOM	Institute for Security and Open Methodologies.
ISO	International Organisation for Standardisation, an organisation that publishes international standards.
ITS	Information Technology Services, a division within the University responsible for is responsible for the provision, maintenance, and support of information and communication technologies within the University of Otago.
OWASP	The Open Web Application Security Project.
Policy	A course of action or principle adopted by an organisation; a business statement of intent, setting the tone for an organisation's culture and defining a management expectation.
Risk	An uncertain event or set of events which could, should it occur, have an effect on the achievement of objectives.
Risk appetite	An organisations unique attitude towards risk taking, which in turn dictates the amount if risk it considers is acceptable.
RMF	The University's Risk Management Framework
SDLC	Systems Development Life Cycle, used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, deploying, and operating an information system.
SIEM	Security Information and Event Management – typically a complex system that takes in log and other data and applies logic to do real time analysis and alerting for security events.
TSO	The Stationery Office is the official publisher and the distributor for UK Government. They also publish corporate governance, ITIL and Prince2 methodologies, standards, and best practice documentation.