

CHARTING YOUR COURSE.

# CYBER SECURITY GOVERNANCE.


Through governance, boards and senior executives play a critical role in creating a cyber resilient organisation.

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government





# The NCSC's Charting Your Course series of documents provides six steps for organisations to improve cyber security governance.

Every organisation's journey toward cyber resilience will be different; these steps provide a general direction of travel. Navigating the individual complexities of governance requires leaders to chart their organisation's own course.

The terms cyber resilience and cyber security are both used in Charting Your Course. Cyber resilience is suggested as a realistic goal for an organisation; rather than focusing primarily on prevention of cyber incidents, resilience also emphasises the importance of recovery and response. Cyber security is primarily used to describe the discipline or practice of protecting the confidentiality, integrity and availability of information assets and systems.

# WHAT IS CYBER SECURITY GOVERNANCE?

Governance is a set of activities that enables organisations to make sound cyber security decisions. The steps outlined in Charting Your Course provide an overview of governance activities, such as defining the principles of a cyber security programme, providing a holistic view of risk, and actively monitoring performance. The governance function sits with boards and senior executives, who can ensure the right cyber security investment is made, at the right time and in the right place.

## Why have Cyber Security Governance?

Clearly defined cyber security governance allows organisations to maximise the benefits of operating in a digital economy. Effective cyber security governance supports the success and sustainability of digital business transformation. Without good cyber security governance, organisations will find it increasingly difficult to ensure basic business continuity or maintain the confidence of external stakeholders.

The outcomes of effective cyber security governance are:

- A cyber security vision that guides the decision-making process across the entire organisation, in line with the overall strategy.
- Well-defined and assigned cyber security roles and responsibilities that are integrated within the organisation.
- A holistic approach to risk management that incorporates cyber security risk, and an improved understanding of the cyber threats faced by the organisation.
- Oversight and allocation of resources through a cyber security forum and cyber security programme.
- A robust system for measuring and reporting compliance and continuous improvement.

# WHO ARE THESE DOCUMENTS FOR?

The responsibility for improving cyber security governance sits at the highest level in an organisation. Charting Your Course often refers to the board of directors but, depending on your organisation, it may be the chief executive or the owner of the company.

Accountability for cyber security sits at the top of an organisation because cyber security outcomes affect the entire business. The board is also best positioned to manage competing risks and align cyber security with other business activities. The board should monitor the investment in—and impact of—cyber security activities, enabled by metrics and reporting provided to them.

Below the board level, executive management guides the organisation's policies and strategies. Nominated security leaders then take responsibility for the delivery of a cyber security programme and the development of controls. The implementation of controls is managed by internal teams along with external specialist support.

A steering committee can include representatives from each organisational layer, and this is often the best method for an organisation to collectively deliver the cyber security programme.



Figure 1: An overview of the six cyber security governance steps.

## STEP 1

### Building a Culture of Cyber Security

A positive cyber security culture of awareness and accountability is driven by the board. The existing culture should be recognised, but influenced by a demonstrated commitment to achieving cyber resilience. The development of a cyber security strategy can promote cultural change, showing the relationship between the organisation's vision and cyber security. A positive cyber security culture also includes supporting everyone in the organisation to play their part in protecting the confidentiality, integrity and availability of the organisation's information assets and systems.

## STEP 2

### Establishing Roles and Responsibilities

Achieving effective cyber security governance requires defining and establishing the organisation's cyber security roles and responsibilities. After they are created, consider at what level in the organisation they need to be performed.

In smaller organisations, most cyber security functions may fall to a single person. In such cases, it is even more important for senior leaders to ensure cyber security duties are realistic, clearly understood, and well-communicated. Everyone in the organisation should understand their role in supporting effective cyber security.

## STEP 3

### Holistic Risk Management

Effective risk management is a core component of governance and must be embedded within the organisation. A framework is needed to effectively identify, analyse, evaluate, and manage cyber security risks. The framework supports consistent decision-making and prioritisation within an organisation, maximising the benefit of investment in cyber security. If an existing risk framework or methodology exists, cyber security should be aligned to this framework.

## STEP 4

### Cyber Security Collaboration

Translating a cyber security strategy and vision into action requires the buy-in and support of the wider organisation. This can be achieved by establishing a committee containing key stakeholders from across the business. The main objective of the steering committee is to achieve consensus and align cyber security priorities with the organisation's objectives. Steering committees are most effective when they contain representatives who can make decisions on resource allocation, prioritisation, and direct cyber security activities.

## STEP 5

### Create a Cyber Security Programme

Organisations should establish a measurable cyber security programme. The programme translates the strategy into action, driving initiatives and continuous improvements in cyber resilience. The steering committee oversees the cyber security programme.

## STEP 6

### Measuring Resilience

The effectiveness of cyber security activities should be accurately measured, assessed and reported. These actions indicate the current cyber resilience of an organisation and progress made through the cyber security programme. Measurement and reporting are vital to good governance, enabling informed decision-making and sustainable investment in cyber security.

“Everyone in the organisation should understand their role in supporting effective cyber security.”



## GOVERNANCE STEP ONE:

# BUILDING A CULTURE OF CYBER RESILIENCE

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government

Organisations must develop a culture of cyber resilience. Everyone in the organisation should feel supported to make decisions that protect the confidentiality, integrity and availability of information assets and systems. Awareness of and accountability for cyber resilience should be seen throughout the organisation as an important and complementary part of that organisation's mission.

Establishing an organisation's cyber security culture occurs from the top down. The board must demonstrate a commitment to cyber resilience. This can be communicated and reinforced through strategy, policy and standards.

## Cyber Resilient Culture

The board has a duty to identify the organisation's key assets and provide strategic direction to the leadership team. If information technology is a key asset or contributes to the organisation's strategic direction, then cyber security should be on the board's agenda.

Ensuring the board's awareness of cyber security is a critical first step towards building a cyber resilient culture. Cyber security is a complex and often technical subject. However, for the board, expressing cyber security in a more familiar business language is advantageous.

Health and safety provides a useful comparison with cyber security for boards. The board does not need to grapple with medical diagnoses to understand the business impact of a health and safety incident. Boards are also interested in more than just incidents; evaluating near-misses, where an organisation gets close to experiencing a security breach, can provide useful insights into current levels of cyber resilience.

A supportive culture in which emerging risks, near-misses, and actual incidents are reported and addressed is fundamental to cyber resilience. Boards should demand strong situational awareness with which to support timely decision-making. It should not require a major incident to make the board aware of the cyber security resilience of the organisation.

“Setting an organisation's cyber security culture is something that happens from the top down and should recognise an organisation's existing culture.”



## Cyber Security Strategy

A strategy is a foundational document because it aligns cyber security with wider organisational objectives. Business and cyber security outcomes depend on the same people, processes and technology — a strategy addresses this relationship for the organisation's specific context.

Part of that context is the organisation's operating environment. External factors will differ in their influence on the organisation's approach to cyber security. Some organisations might have higher regulatory or compliance considerations, while others will have a more diverse threat landscape. Internal factors also differ, from insider threats to key business partners or third-party dependencies.

“A strategy should allow for and recognise key business objectives and provide guidance on how they can be achieved securely.”

## Policies & Standards

Policies and standards provide further guidance to an organisation on establishing a culture of cyber resilience. Write these policies and standards in a tone that represents the current culture of the business; they should lead the organisation on a pathway to cyber resilience, rather than trying to transform it by writ.

Policies and standards need not be long or overly complicated; it is most important for them to be clear. This usually starts with creating a cyber security policy but can be extended to include policies addressing issues such as privacy, data governance, and acceptable usage. These policies will have a wide audience, so it should be easy to interpret and implement them.

Where policies do not provide specific detail, they can be further defined by standards. Standards are also mandatory, but may change more often than the policies they support to keep pace with technology.

There are many frameworks available to guide the creation of policies and standards, including the New Zealand Information Security Manual (NZISM), ISO27001, or Center for Internet Security (CIS) Critical Security Controls.

## GOVERNANCE STEP TWO:

# ESTABLISHING ROLES & RESPONSIBILITIES

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government

Clearly defining an organisation's cyber security roles and responsibilities—and establishing who is best suited to performing them—is the second step to achieving effective cyber security governance.

Staff numbers in smaller New Zealand organisations can make the separation of duties difficult, and cyber security responsibilities may fall upon a single person. In all cases, it remains important to ensure duties are realistic, clearly understood, and well-communicated.

## Board of Directors

The board of directors is ultimately accountable for an organisation's corporate governance. Members of the board provide strategic direction and communicate the organisation's cyber security principles. The board should:

- Set the strategic cyber security direction of the organisation.
- Assist prioritisation by helping to identify critical assets and highlighting key risks.
- Assess the effectiveness of the cyber security strategy. This should include:
  - Consideration of metrics and reporting.
  - Reviewing audits and cyber security tests.
  - Reviewing cyber security incidents and near misses.

**Note:** These accountabilities are not included in the RASCI model (see page 14) as they cannot be delegated or passed to anyone else and must be carried out by the board.

## Executive Management

The executive management team is responsible for ensuring the implementation of the cyber security strategy. In organisations with flat management structures or with small teams, executive management may not exist as a formal layer. However, these functions should be performed regardless. For those who are both a board member and chief executive, it's important to separate these functions when possible. Executive management should:

- Realise the board's cyber security strategy.
- Provide resourcing to deliver the strategy.
- Approve relevant policies and standards.
- Measure the effective delivery of the cyber security programme.

“Everyone in the organisation should understand their role in supporting effective cyber security governance and resilience.”

## Chief Information Security Officer (CISO) / Chief Cyber Security Officer

The CISO is responsible for cyber security requirements at the executive level. They typically lead a security team or manage a virtual team through a distributed security function leveraging resources from other teams in the organisation. It is impossible for the CISO to 'own' every aspect of security, since some functions will be dependent on other parts of the business. The finance, legal, human resources, physical security, and infrastructure management teams all work closely with the CISO to enable them in their role.

**Note:** The CISO title itself is less important than the fact that the responsibilities of this role are assigned and that there is a direct link with the executive leadership team.

The CISO is accountable for representing cyber security in the organisation. A programme of continuous improvement lead by the CISO will ensure a focus on cyber security. This can be achieved by:

- Developing and maintaining cyber security policies and standards.
- Providing guidance and leadership on cyber security procedures and guidelines.
- Developing a cyber security strategy, architecture, and risk management process.
- Managing the budget and funding for the cyber security programme.
- Implementing cyber security awareness and training.
- Proactively maintaining the confidentiality, integrity and availability of information assets.
- Providing guidance on best practice, including infrastructure configuration and application development.
- Assessing the cyber security implications to the business of the adoption of new technologies or services.
- Guiding the business on the potential consequences and impacts of threats.
- Acting as the point of contact for cyber security.
- Chairing the cyber security steering committee.
- Assessing and providing recommendations on any exceptions to policies or standards.
- Coordinating audit and assurance activities.

## Information Security Manager (ISM) / Cyber Security Manager

The ISM focuses on the delivery and operational management of cyber security. Many organisations choose to combine the roles of CISO and Information Security Manager, but ideally these should be separated. This allows the CISO to focus on the governance and strategic aspects of cyber security, especially if combined as part of a larger executive role.

The ISM's typical responsibilities include:

- Managing and coordinating the response to cyber security incidents, changing threats, and vulnerabilities.
- Developing and maintaining cyber security procedures and guidelines.
- Providing guidance on cyber security risks introduced from business and operational change.
- Managing the life cycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning.
- Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications.
- Providing input and support to regulatory compliance and assurance activities, and managing any resultant remedial activity.
- Developing a metrics and assurance framework to measure the effectiveness of controls.
- Providing day-to-day management and oversight of operational delivery.

Some larger organisations may also have a Cyber Security Operations Manager or Technical Security Manager position. These roles would take on some of the more technical duties from the ISM and be more actively involved in the day-to-day running of cyber security operations.

“Everyone in the organisation should understand their role in supporting effective cyber security governance and resilience.”



## The RASCI Model

The recommended method for defining cyber security roles and responsibilities is to use the RASCI model. The acronym is an abbreviation for the following:

**Responsible:** The role or team assigned to undertake a task. There should be at least one role with primary responsibility, but others can provide support.

**Accountable:** The role that ultimately approves the activity and ensures that it is carried out end to end. There must be one role that is accountable for each specified task or function.

**Supporting:** The roles and teams that support the responsible and accountable individuals in completing the activity.

**Consulted:** The stakeholders who need to be formally consulted regarding the activity, and who may provide input and feedback.

**Informed:** The stakeholders who need to be kept informed about the progress of the activity.

The RASCI model can be used to create a simple table that defines each activity and assigns it to an individual or role. This document provides an example for your organisation to use and describes key roles.

The Roles & Responsibilities guide is intended to be used as part of NCSC's wider *Charting Your Course* six steps guides.

## Applying the RASCI Model: A Practical Example

The RASCI model on the next page associates cyber security activities with key roles. This provides a practical example of the RASCI roles outlined above. The model can also be inverted, with RASCI along the top and names of those responsible in the cells.

You can apply this model to your organisation. Organisations may differ in their application of RASCI to cyber security roles, and the example below is not a perfect blueprint for every organisation.

“If you are unsure who performs a specific function, or if someone is unaware they have been assigned to a function, it may not be getting done.”

## Roles and Responsibilities

Activity	Responsible	Accountable	Supporting	Consulted	Informed
A central point of contact for internal and external parties on information and cyber security.	CISO	Executive management	ISM		Board of directors
Builds board and executive level awareness of cyber security risks and threats to the organisation.	CISO	Executive management	ISM	Other business units and subject matter experts	Board of directors

### Cyber Security Strategic Alignment

Establishes and embeds the required cyber security culture.	Executive management	Board of directors	CISO	Cyber security steering committee	All staff
Provides strategic cyber security direction and advice to the board.	Executive management	Board of directors	CISO	ISM	
Interfaces with the board/executive management on strategic security initiatives and provides feedback.	CISO	Executive management	ISM	Other business units and subject matter experts	
Defines and implements information and cyber security strategies.	CISO	Executive management	ISM	Cyber security steering committee	Board of directors
Budgeting and acquisition of security funding.	CISO	Executive management		Cyber security steering committee	Board of directors
Provides security leadership in cross-functional business and security teams.	CISO	Executive management	ISM		
Develops and maintains cyber security architecture.	ISM	CISO		Other business units and subject matter experts	Executive management
Defines relevant cyber security regulatory and compliance requirements.	Executive management	Board of directors	CISO	Legal counsel	ISM

Activity	Responsible	Accountable	Supporting	Consulted	Informed
<b>Cyber Security Risk Management</b>					
Defines and embeds cyber security risk appetite and tolerances.	Executive management	Board of directors	CISO	ISM	
Establishes and implements a cyber security risk management framework.	CISO	Executive management	Subject matter experts	Board of directors	Other business units
Identifies, assesses and mitigates cyber security and IT risks for business activities and projects.	ISM	CISO		Cyber security steering committee	Executive management
Manages cyber security risk escalations and their approvals.	ISM	CISO		Cyber security steering committee	Executive management
Develops, maintains, and publishes an information security framework.	CISO	Executive management	ISM	Cyber security steering committee	
Develops, maintains, publishes, and enforces cyber security policies.	CISO	Executive management		Cyber security steering committee	
Develops, maintains, publishes, and enforces information security standards.	ISM	CISO		Cyber security steering committee	Executive management
Develops, maintains, publishes, and enforces security processes according to security standards.	ISM	CISO			Cyber security steering committee

Activity	Responsible	Accountable	Supporting	Consulted	Informed
----------	-------------	-------------	------------	-----------	----------

### Cyber Security Programme

Develops and implements appropriate changes to the security programme.	ISM	CISO	Programme management office	Cyber security steering committee	Executive management
Develops and implements a renewable security awareness programme.	ISM	CISO		Cyber security steering committee	
Develops and maintains a cyber security roadmap.	ISM	CISO	Programme management office	Cyber security steering committee	Executive management
Develops and delivers cyber security performance metrics.	ISM	CISO		Cyber security steering committee	Executive management
Implements, operates and maintains a continuous security assurance process.	ISM	CISO	Third party auditors and service providers	Cyber security steering committee	Executive management

### Cyber Security Operations

Develops, implements, maintains, and monitors security technologies according to security standards.	ISM	CISO	Third party service providers	Other IT architecture and operations teams	
Develops, maintains, publishes, and enforces operational procedures (including hardening configurations).	ISM	CISO		Other IT architecture and operations teams	
Implements security changes and remediation to business systems and applications.	ISM	CISO	Other IT operations and project teams		
Ongoing assessment and review of cyber threat intelligence sources and information.	ISM	CISO	Third party service providers		Executive management Cyber security steering committee

Activity	Responsible	Accountable	Supporting	Consulted	Informed
Oversight and management of vulnerability scanning, analysis and remediation.	ISM	CISO	Other IT operations and project teams		
Management of security in the operating environment on a day-to-day basis.	ISM	CISO	Other IT operations and project teams	Third party service providers	
Management of security incidents and taking action in response.	ISM	CISO	Other IT operations and project teams	Third party service providers	Executive management
Monitors trends in capacity and performance of cyber security technologies.	ISM	CISO	Other IT operations and project teams		Cyber security steering committee
Approves security changes in change advisory/control boards.	ISM	CISO		Other IT operations and project teams	
Provides and reports on continuous security assurance according to security standards.	ISM	CISO	Third party service providers		Executive management Cyber security steering committee
Coordinates IT audit activities and management response.	ISM	CISO	Other IT operations and project teams	Other business units	Executive management
Reviews access, entitlement and provisioning for users.	ISM	CISO		Other business units	



GOVERNANCE STEP THREE:

# HOLISTIC RISK MANAGEMENT

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government

“Effective risk management is a core aspect of governance and must be embedded within the organisation.”

## Risk Alignment and Management

Cyber security will support the resilience of a broad range of business processes. Risk is therefore best considered at a holistic level, where the interdependencies of processes can be understood. In most organisations risk management frameworks may already exist for areas such as health and safety. Cyber security risk should align with these existing frameworks. Alignment enables consistency of risk management, but also frames cyber security in a familiar way for the wider organisation.

The organisation's risk framework must clearly express its risk appetite and tolerance. It is ultimately the board that must provide this direction; without this, risk management cannot be effectively implemented. The framework should take into account the organisation's culture, as well as any legal or regulatory requirements. The organisation's appetite and tolerance for risk will affect how that risk is managed. For example, an organisation with a greater risk appetite may require more regular oversight and proactive monitoring of risks to ensure they remain within defined tolerances.

Operating a cyber security risk management framework enables organisations to enhance their risk awareness. Regardless of risk appetite, investment in developing a framework supports the organisation's pursuit of strategic objectives. Once a cyber security risk framework is established and aligned, the risks themselves need to be managed to within the levels and tolerances defined as acceptable.

“Cyber security risk management must align with the organisation's existing risk framework.”

## Managing Cyber Security Risk

Consistent management of an organisation's cyber security risks requires planning and preparation. The organisation must have a good understanding of its key business assets and the consequences for the business if the confidentiality, integrity or availability of those assets is compromised.

Adopting a formalised risk management framework will help the organisation produce consistent and repeatable outcomes. By using an established standard such as ISO 31000:2018 or NIST SP 800-30r1, the organisation can evaluate threats, vulnerabilities and consequences within the context of business objectives. These standards also serve as a basis for achieving a suitable and agreed way to respond to the risk.

### Scope

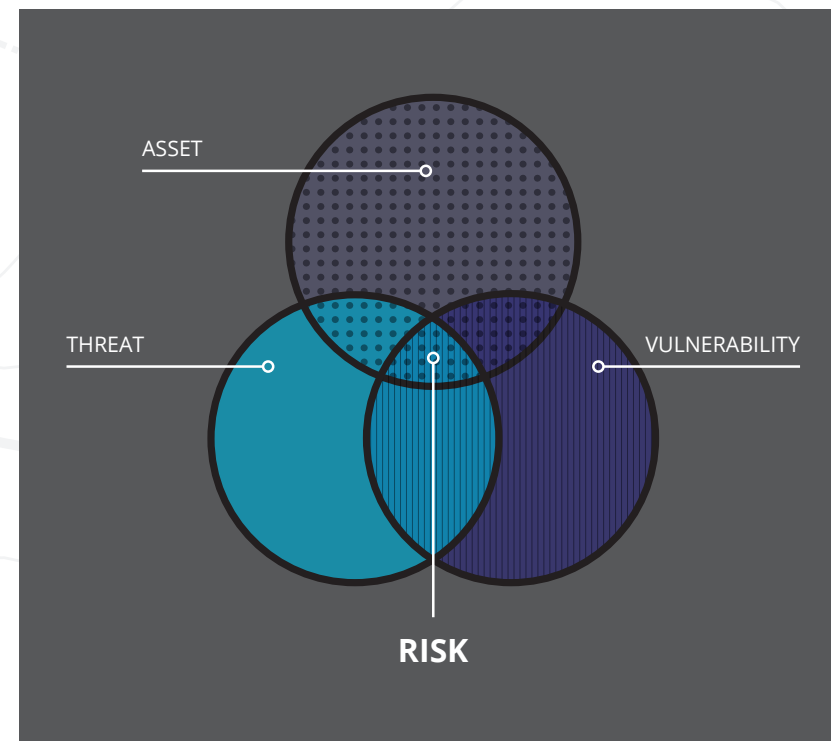
Defining the scope of a risk assessment makes it more achievable. The scope should be based on agreement within the organisation of the assets to assess, as well as defining the people, processes and technologies in focus.

Tangible assets are often first to mind, but it is also important to consider intangible assets such as reputation or intellectual property. Also consider how an asset is utilised to generate business value: for example, assets that are not needed on a daily basis but perform critical monthly, yearly or intermittent disaster recovery functions.

## Threat and Vulnerability Identification

Effective assessment of risk requires maintaining an awareness of threats and vulnerabilities, both current and emerging, which may impact the business. Cyber security risk arises when a threat exists that can exploit a vulnerable asset. Where a threat is present without vulnerability, or vice versa, the risk will be lower. The threats and vulnerabilities relevant to an organisation are determined by the assets it employs.

**Figure 1 Identifying Risk**



## Threats

The impact of threats can be better understood by reviewing threat trends and reporting across industry sectors. This information can provide insight into the likelihood that the organisation may be affected by a cyber security breach.

A threat taxonomy will help to consistently classify and describe threats. The taxonomy will likely include internal and external threat actors and adversarial, accidental, structural, and environmental threats.

## Assets and Vulnerability

It is difficult to perform a meaningful assessment of risk without an understanding of the organisation's key assets. Maintaining a database of IT systems that process, store and transport the organisation's critical information will enable the assessment of vulnerabilities. This database will provide a clear understanding of possible points of compromise by the identified threats.

## Assessment and Evaluation Method

Risk assessment can be performed using a number of methods. The process principally involves some level of quantitative or qualitative analysis. This analysis categorises the level of risk likelihood and the potential business impact, which is expressed in financial, reputational, legal, or operational terms.

Objective evaluation of risk using quantitative methods yields an assessment based on concrete figures. This requires data sourced from the organisation to calculate the annualised loss expectancy (ALE) or value at risk (VAR).

Assessing risk using semi-quantitative and qualitative methods provides a useful but more subjective outcome. These methods may be used when there are few figures available, or when a quantitative assessment is too demanding. In order to assess risk, these approaches still require defined measures of likelihood and consequence; these are often presented as a band with an upper and lower limit.

When a risk is identified, its management should be allocated to an individual in the relevant area of the organisation. The risk owner requires the knowledge to evaluate the impact to the organisation and the ability to provide the required response. This evaluation and response to risk also requires a uniform process to ensure that any risks outside the tolerance of the organisation are consistently treated and managed.

## Risk Response and Ongoing Management

Any risks identified from an assessment must be managed in accordance with the organisation's risk tolerance. All risks should be recorded in an internal risk register. The identified risk owner is responsible for the ongoing management and reporting of the risk, and assessing the recommended methods to treat the risks.

Risk responses can take a number of different approaches, but are usually categorised as the following:

- **Risk acceptance:** the risk owner can elect to accept the level of risk.
- **Risk reduction:** the risk is reduced to an acceptable level through applying controls.
- **Risk transfer:** the risk is transferred to another party to mitigate the impact. This is usually done through insurance.
- **Risk avoidance:** the business avoids activities that have given rise to the risk.

One or more of these approaches may be adopted and often will require the risk to initially be reduced and then either accepted or transferred.

Ongoing risk management outputs should be reported to all levels of the organisation. The use of risk metrics and dashboards can illustrate risk levels and changes (refer to Governance Step Six: Measuring Resilience and Compliance for further information). This supports clear and effective communication, thereby facilitating decision-making and

providing clarity and prioritisation for driving improvement through the organisation's cyber security programme.

“If the organisation lacks a risk framework, one must be established before cyber security risk can be effectively identified, evaluated and managed.”



#### GOVERNANCE STEP FOUR:

# CYBER SECURITY COLLABORATION

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government

Successfully translating a cyber security strategy and vision into action requires the wider organisation's support. This can be achieved by establishing a committee and a working group containing key stakeholders from across the business.

A steering committee should include representatives who can make decisions that resource, prioritise and direct cyber security activity. The primary objective of the steering committee is to achieve consensus and align cyber security priorities, risks, initiatives, and resourcing with the organisation's objectives.

## Cyber Security Steering Committee

Scheduling periodic steering committee meetings is a good way to enable discussion of cyber security issues affecting an organisation. These meetings help to align the cyber security programme and its deliverables with organisational business objectives. Where an organisation lacks depth in cyber security knowledge, the meetings can also be an opportunity to improve understanding. A by-product of this approach is increased cyber security awareness and buy-in to decisions that have been made to address risks.

Key responsibilities for the cyber security steering committee are:

- Reviewing the cyber security strategy and ensuring that it aligns with and is supported by the wider organisation.
- Identifying and discussing new or emerging cyber security risks, threats, practices, or compliance issues.
- Providing direction on the effectiveness and efficiency of cyber security initiatives, and ensuring they support business operations.
- Identifying organisational changes, gaps, or critical business processes where additional integration and cyber security focus is required.
- Ensuring adequate funding and resourcing is allocated to the cyber security programme.
- Leading by example and embodying the behaviours that reflect the desired cyber security culture for the organisation.

In small organisations, the steering committee may be compromised of individuals who already meet regularly. It is still important to set time aside to meet specifically as the cyber security steering committee. Providing a standing agenda is a useful way to focus the conversation, and can be developed based on the guidance in this document.

## Cyber Security Working Group

While a steering committee can be effective at translating the strategic context into priorities, it may only meet once per month or less. At an operational level, a more hands-on cyber security working group should be established. This group should meet frequently, actively participate in the cyber security programme, and oversee task completion. The cyber security working group should:

- Deliver the outcomes agreed by the steering committee.
- Be represented by line management, operational, and delivery teams.
- Cover the initiatives included in the cyber security programme.
- Be aware of all activities to create, improve or maintain cyber security controls, including people, process, or technology initiatives.
- Review any cyber security risks and issues raised by the business.
- Review any incident reports and near-misses associated with cyber security.
- Review any cyber security testing, including disaster recovery, business continuity, penetration tests, and incident response.

“Translating the cyber security strategy and vision into action requires the buy in and support of the wider organisation.”

GOVERNANCE STEP FIVE:

# CREATE A CYBER SECURITY PROGRAMME

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government

“The goal of a cyber security programme is to ensure that any investment in cyber security provides the best possible improvement in cyber resilience, as defined by the strategy.”



## Cyber Security Programme

The delivery of cyber security initiatives is usually achieved through a security programme. To maintain focus and priority, a dedicated cyber security programme is recommended. Some organisations may deliver cyber security initiative as part of larger infrastructure programmes, or spread these initiatives across business units.

A key function of the security programme is the lifecycle management of any deployed cyber security technologies. Without maintenance, systems and capabilities will rapidly lose their effectiveness and may not provide the intended outcomes.

Delivery of the programme can be achieved by allocating in-house resources or contracting external specialists. This process requires skillsets across cyber security architecture, design, and deployment. An understanding of the organisation's operational processes and management is also necessary.

It is important that the initiatives of a cyber security programme are aligned to an organisation's cyber security strategy and address the risks identified in the business. These initiatives include items such as awareness training, policy development, and deploying security systems.

## Cyber Security Architecture

A cyber security architecture provides a blueprint for the cyber security programme. Cyber security architecture should help both delivery and operational teams to carry out their functions with clear direction on how to meet the security requirements of the organisation. In large organisations, cyber security architecture can become complex and may be encompassed within many documents.

At minimum, a cyber security architecture can provide clear principles on how the organisation manages cyber security. These principles could provide guidance on areas such as building secure IT systems and software, investing in security solutions and services, managing the risk of cloud services, partnering with third parties, or securely deploying systems and code.



## Cyber Security Roadmap

Developing a cyber security roadmap supports the delivery of the cyber security programme through prioritising the objectives and goals defined in the cyber security strategy. The roadmap will provide clear guidance as to the required sequence of tasks and deliverables by specifying what, when, who, and how the initiatives will be delivered as part of the cyber security programme.

## Controls Framework

It is beneficial to have a framework that identifies and links controls to the outcomes they are intended to achieve. Controls underpin all cyber security initiatives and can be comprised of people, processes or technology. They should be mapped to the policy and compliance outcomes of the organisation. A common framework used by organisations is the NIST Cybersecurity Framework, which groups all controls into 'Identify, Protect, Detect, Respond and Recover' categories.

“It is important that the initiatives of a cyber security programme are aligned to an organisation's cyber security strategy and address the risks identified in the business.”



## GOVERNANCE STEP SIX:

# MEASURING RESILIENCE

NATIONAL CYBER SECURITY CENTRE  
A PART OF THE GCSB



New Zealand Government

Reporting provides stakeholders with assurance that the organisation is cyber resilient and delivers evidence of a return on investment in cyber security activities. Measurement and reporting are the basis for continuous improvement in the cyber security programme.

“The effectiveness of all cyber security activity should be accurately measured and reported.”

## Measuring and Reporting Cyber Resilience

Measures should be defined for all controls and aligned to a cyber security framework. This task should include a clear definition of effectiveness that can be reliably measured and reported on. For example, using the latest operating system version is a control that can be measured by the number of systems upgraded.

The effectiveness of the controls and the overall level of compliance must be reported back to the organisation and any relevant stakeholders on a regular basis. The accountability for this reporting should be clearly defined as part of *Governance Step Two: Establishing Roles and Responsibilities*.

Controls can be evaluated using a combination of internal and external methods, such as:

- self-assessment
- internal review
- penetration testing
- security audit
- independent review

## Metrics and Indicators

Metrics and indicators are used as support tools to inform decisions that enable the business to operate effectively. Metrics provide consistent tracking of the effectiveness of an organisation's cyber security programme. For example, to stay within acceptable risks levels, an organisation might define a time period within which all operating systems must be upgraded to the most recent version. Reporting will display the organisation's progress in upgrading, relative to the time constraint.

Indicators are quantitative or qualitative measures that anticipate future events. From a governance perspective, useful metrics and indicators should provide ongoing insights into evolving trends, risks and behaviours, as well as highlighting any required changes in strategy and risk tolerance, or the need for further investment.

Developing meaningful metrics and indicators in the early stages of any cyber resilience initiative is important. This task provides an agreed and consistent method of measurement across the organisation, and can demonstrate the effectiveness of investments in a cyber security programme.

“All metrics should follow the SMART model: Specific, Measurable, Achievable, Relevant, and Time-bound.”

## Assurance

This term is used for the method of providing confidence in the effectiveness of the controls defined as part of a cyber security framework. There are many methods of providing assurance, and a combination of these should be used. Four common methods are:

**Self-assessment:** In this method, either the cyber security team (as defined in Cyber Security Governance Step Two: Establishing Roles and Responsibilities) or other groups within the organisation assess and report on the effectiveness of controls. This could be as simple as advising on the number of people who have access to a system. This method is generally quite subjective and relies on the integrity of the individuals performing the assessment to ensure their findings are valid.

**Internal Assessment:** Many larger organisations have staff that provide assessment services, such as internal audit teams. These teams need not be focussed on cyber security but can be leveraged to assist with this function when required.

**External Assessment:** External assessment can take many forms, including independent controls framework assessments against industry standards, regulatory and compliance audits, table-top exercises to simulate a breach, and penetration tests to understand points of vulnerability.

**Automated Assessment:** In-built testing, monitoring and reporting of the effectiveness of controls is the ultimate goal when building assurance. This may not be possible for all controls, but identifying and selecting systems and tools that dynamically evaluate and report on security compliance and overall resilience provides an ongoing and real-time level of assurance.

Regardless of the assurance method used, it is important that each one references the same framework and uses agreed metrics. If internal and external assessment teams use different methods or measures for assessment, confusion may arise around the prioritisation and focus of the cyber security programme.

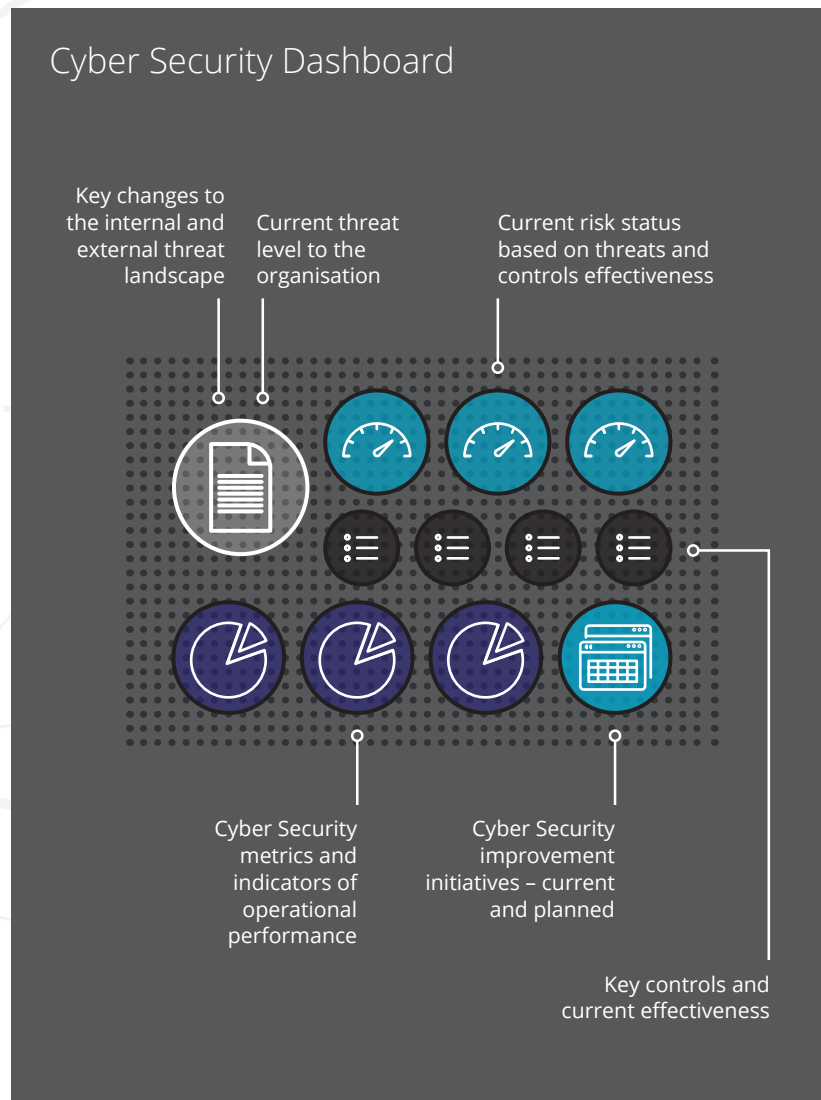
## Reporting

Many assessment methods provide reporting as part of their function. Examples include audit reports, independent assessments, penetration test reports, and red team reports. Additionally, operational and performance reporting is produced by internal teams and third parties. These reports may include event and incident details, as well as identified risks.

All of this information should be reported to the organisation in a cohesive fashion using a summarised dashboard. A dashboard allows the business to visualise risks and their associated threat levels. They also provide a collective displays of improvements outlined in the cyber security programme as they are delivered.

A cyber security dashboard could include the following metrics and indicators:

- The current overall threat level to the organisation.
- Internal and external threat landscapes, and any notable changes in these.
- Operational cyber security metrics and indicators of operational performance.
- The current risk status based on threats and control effectiveness.
- Current and planned cyber security initiatives.





The New Zealand Information Security Manual (NZISM) and Protective Security Requirements (PSR) contain standards and guidance related to governance. While every effort has been made to align *Charting Your Course* with the PSR and NZISM, where difference is found, they remain the authoritative standard for mandated agencies.