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

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

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.

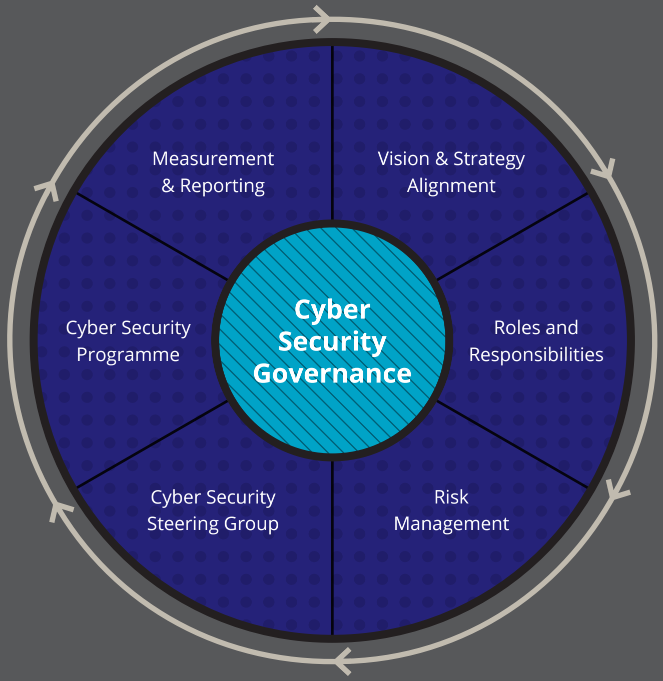
Cyber Security Governance
Vision & Strategy Alignment
Roles and Responsibilities
Risk Management
Cyber Security Steering Group
Cyber Security Programme
Measurement & Reporting

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.”

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.