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 4) 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.

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

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.

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
Cyber Security Risk Management					
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	

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.