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."

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.