GOVERNANCE STEP FOUR:

CYBER SECURITY COLLABORATION

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.

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

New Zealand Government

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.”

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.