GOVERNANCE STEP THREE:

HOLISTIC RISK MANAGEMENT

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

> “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

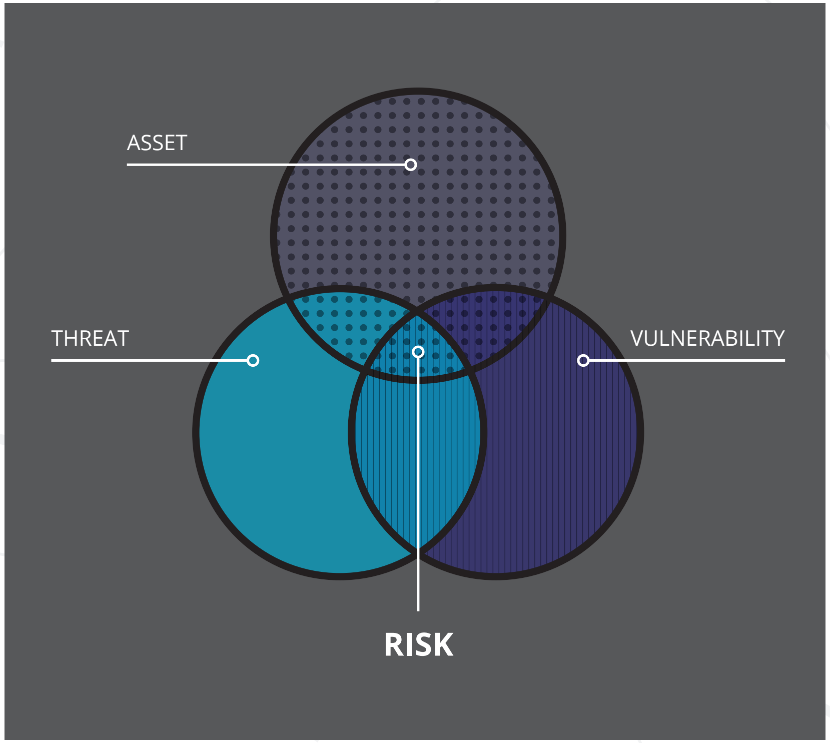
Defining the scope of a risk assessment makes it more achievable. The scope should be based on agreement within the organisation of the assets to assess, as well as defining the people, processes and technologies in focus.

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.”

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.