GOVERNANCE STEP SIX:

MEASURING RESILIENCE

Reporting provides stakeholders with assurance that the organisation is cyber resilient and delivers evidence of a return on investment in cyber security activities. Measurement and reporting are the basis for continuous improvement in the cyber security programme.

NATIONAL CYBER SECURITY CENTRE
A PART OF THE GCSB

New Zealand Government

> "The effectiveness of all cyber security activity should be accurately measured and reported."

Measuring and Reporting Cyber Resilience

Measures should be defined for all controls and aligned to a cyber security framework. This task should include a clear definition of effectiveness that can be reliably measured and reported on. For example, using the latest operating system version is a control that can be measured by the number of systems upgraded.

The effectiveness of the controls and the overall level of compliance must be reported back to the organisation and any relevant stakeholders on a regular basis. The accountability for this reporting should be clearly defined as part of *Governance Step Two: Establishing Roles and Responsibilities*.

Controls can be evaluated using a combination of internal and external methods, such as:

- self-assessment
- internal review
- penetration testing
- security audit
- independent review

> "All metrics should follow the SMART model: Specific, Measurable, Achievable, Relevant, and Time-bound."

Metrics and Indicators

Metrics and indicators are used as support tools to inform decisions that enable the business to operate effectively. Metrics provide consistent tracking of the effectiveness of an organisation's cyber security programme. For example, to stay within acceptable risks levels, an organisation might define a time period within which all operating systems must be upgraded to the most recent version. Reporting will display the organisation's progress in upgrading, relative to the time constraint.

Indicators are quantitative or qualitative measures that anticipate future events. From a governance perspective, useful metrics and indicators should provide ongoing insights into evolving trends, risks and behaviours, as well as highlighting any required changes in strategy and risk tolerance, or the need for further investment.

Developing meaningful metrics and indicators in the early stages of any cyber resilience initiative is important. This task provides an agreed and consistent method of measurement across the organisation, and can demonstrate the effectiveness of investments in a cyber security programme.

Assurance

This term is used for the method of providing confidence in the effectiveness of the controls defined as part of a cyber security framework. There are many methods of providing assurance, and a combination of these should be used. Four common methods are:

Self-assessment: In this method, either the cyber security team (as defined in Cyber Security Governance Step Two: Establishing Roles and Responsibilities) or other groups within the organisation assess and report on the effectiveness of controls. This could be as simple as advising on the number of people who have access to a system. This method is generally quite subjective and relies on the integrity of the individuals performing the assessment to ensure their findings are valid.

Internal Assessment: Many larger organisations have staff that provide assessment services, such as internal audit teams. These teams need not be focussed on cyber security but can be leveraged to assist with this function when required.

External Assessment: External assessment can take many forms, including independent controls framework assessments against industry standards, regulatory and compliance audits, table-top exercises to simulate a breach, and penetration tests to understand points of vulnerability.

Automated Assessment: In-built testing, monitoring and reporting of the effectiveness of controls is the ultimate goal when building assurance. This may not be possible for all controls, but identifying and selecting systems and tools that dynamically evaluate and report on security compliance and overall resilience provides an ongoing and real-time level of assurance.

Regardless of the assurance method used, it is important that each one references the same framework and uses agreed metrics. If internal and external assessment teams use different methods or measures for assessment, confusion may arise around the prioritisation and focus of the cyber security programme.

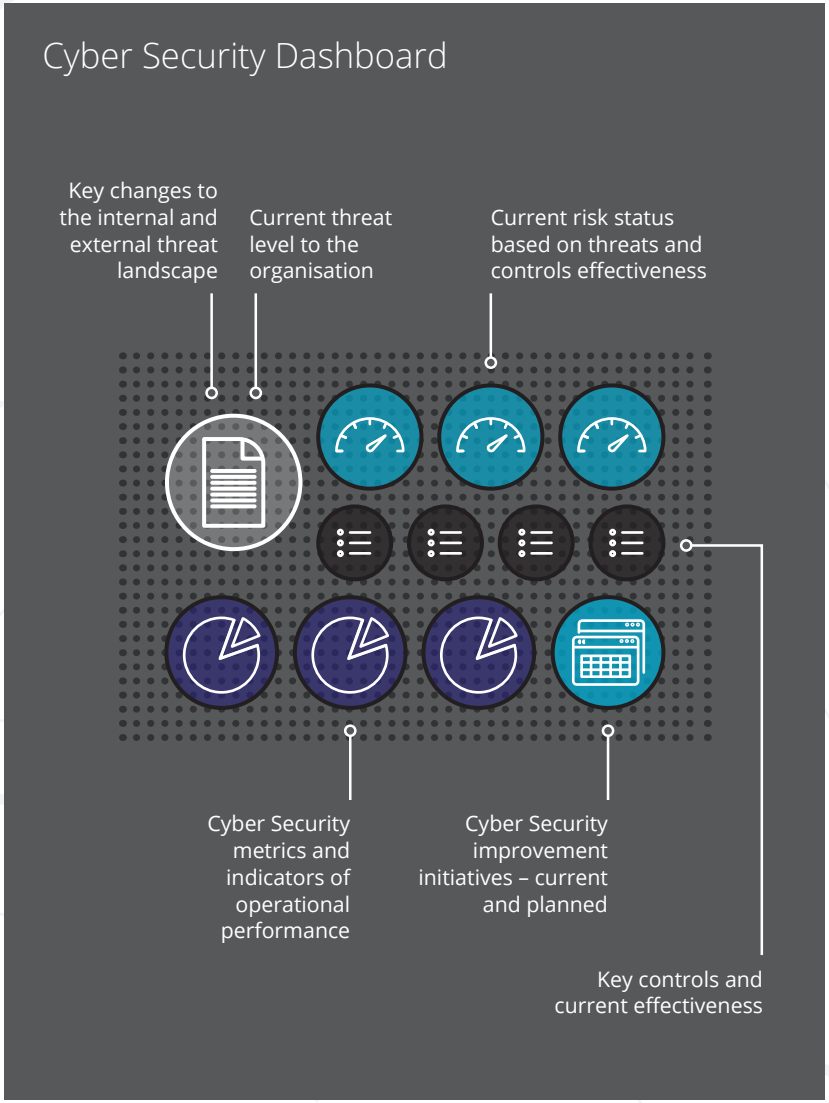
Reporting

Many assessment methods provide reporting as part of their function. Examples include audit reports, independent assessments, penetration test reports, and red team reports. Additionally, operational and performance reporting is produced by internal teams and third parties. These reports may include event and incident details, as well as identified risks.

All of this information should be reported to the organisation in a cohesive fashion using a summarised dashboard. A dashboard allows the business to visualise risks and their associated threat levels. They also provide a collective displays of improvements outlined in the cyber security programme as they are delivered.

A cyber security dashboard could include the following metrics and indicators:

- The current overall threat level to the organisation.
- Internal and external threat landscapes, and any notable changes in these.
- Operational cyber security metrics and indicators of operational performance.
- The current risk status based on threats and control effectiveness.
- Current and planned cyber security initiatives.



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.