28 February 2023

Cyber Security Guidance

National Cyber Security Centre

NCSC Cyber Security Framework

This is a beta release of the NCSC's Cyber Security Framework. The framework sets out how the NCSC thinks, talks about, and organises cyber security efforts. Its five functions represent the breadth of work needed to secure an organisation.

What is a cyber security framework?

Good security practice tells us that security leaders and security governance should use a framework to help manage their organisation's security programme. A cyber security framework complements, but does not replace, an agency's risk management process and cyber security programme.

Figure 1: how a cyber security framework is positioned in cyber security management.

The NCSC uses the framework to shape our guidance, services, system leadership as the Government Chief Information Security Officer, advice to ministers, and our regulatory roles.

This is our demonstration of a good cyber security framework

Under the Protective Security Requirements, every public service department needs to have a cyber security framework.[1] This is our framework, and as the system leader for cyber security we are sharing it to show what we think a good framework looks like.

How the NCSC will use our framework

At the NCSC, we will use the framework across our cyber security efforts.

We will use it to help us think about our services and activities, in relation to how we advise stakeholders, detect threats, deter threat actors, and disrupt cyber actors in order to protect Aotearoa New Zealand.

We will use the framework to understand and prioritise the advice and guidance we provide, and the framework will inform our future plans. An example of this could be determining if we need to produce advice on detection and containment before we provide further advice on incident response.

How you can use this framework

The NCSC recognises that cyber security is a multi-dimensional challenge. We encourage all organisations to have a well-rounded work programme to improve their cyber resilience. A framework helps you do this.

All public service departments need to use a cyber security framework in order to meet their mandatory obligations under the Protective Security Requirements. While this framework has been developed to frame and organise the cyber security activities of the NCSC, it can be used by organisations in any sector. It is intended to be useful to companies, other government agencies, and not-for-profit organisations, regardless of their focus or size.

You could use your current processes and leverage the framework to identify opportunities to strengthen and communicate how you manage cyber security risk while aligning with industry practices. Alternatively, if you don't currently have a cyber security work programme, you can use our framework to establish your programme.

---

[1] See '**Mandatory requirements | Protective Security Requirements(external link)**', and '**Adopt a framework to manage information security | Protective Security Requirements(external link)**' for further information

What is the NCSC framework?

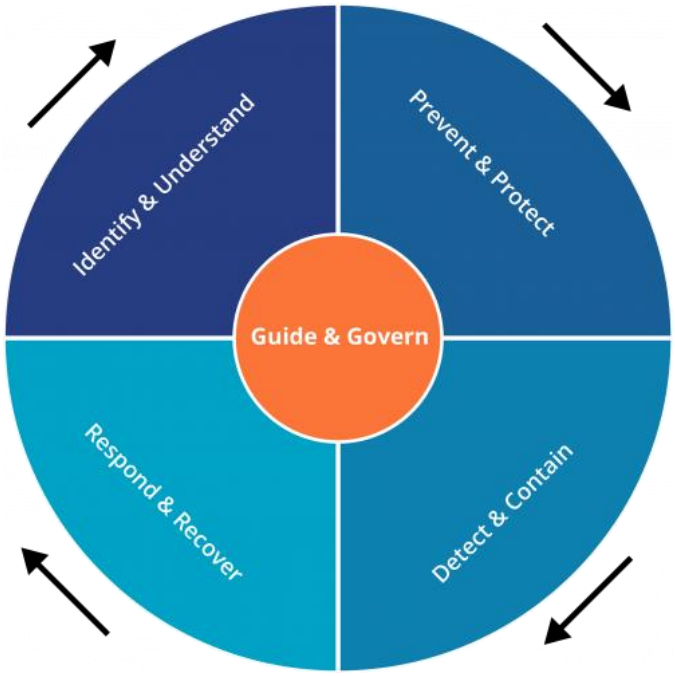
The NCSC Cyber Security Framework (the framework) is composed of two parts:

- **A core set of interrelated, concurrent, and continuous cyber security functions:** Guide & Govern, Identify & Understand, Prevent & Protect, Detect & Contain, and Respond & Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an agency's management of cyber security risk.
- **A set of cyber security outcomes related to each of the functions**. These describe the desirable security outcomes for each function and relate to balancing the management of cyber security risks and delivery to the overarching security and business strategies. Each function has five outcomes.

The framework's five functions are:

1. **Guide & Govern**
   Cyber security is promoted through governance efforts and by providing guidance to your people. Staff are guided and informed on what they need to do to help secure the organisation and its assets.
2. **Identify & Understand**
   We know which cyber security activities we are responsible for and where to apply them. This includes identifying our assets, understanding the context and threat environment we operate in and use those assets in, and knowing where security responsibilities lie between us and our suppliers.
3. **Prevent & Protect**
   We focus on reducing actual risk and seek to incrementally improve now, rather than aiming for perfect security tomorrow. Assets need protection in a way that prevents bad things from happening, and potential vulnerabilities are removed before they are exploited.
4. **Detect & Contain**
   Incidents will occur and they need to be contained. Security monitoring is a necessary component of knowing when abnormal activity is occurring. Knowing how and why our systems interconnect is essential to limiting threat actors' ability to move between systems and gain access to more of our information.
5. **Respond & Recover**
   We prioritise our security incident response to get critical services back to normal operation as quickly as possible.

As a security lifecycle, the five functions can be viewed like this:



Each of these five functions has a series of objectives. These are described in further detail below.

Guide & Govern

Cyber security is promoted through governance efforts and by providing guidance to our people. Staff are guided and informed on what they need to do to help secure the organisation and its assets.

Security objectives

1. We embed security principles and practices across our organisation, so that cyber security supports our organisation's outcomes.
2. Our people do not need to be security experts to use our systems safely.
3. We prioritise our security investments to focus on real threats to our important systems.
4. We continuously invest in improving our security posture and adapting to new and evolving threats.
5. We seek assurance that our security efforts are effective, robust, and adaptable to meet evolving threats.

Identify & Understand

We know the cyber security activities we are responsible for and where to apply them. This includes identifying our assets, understanding the context and threat environment we

operate and use those assets in, and knowing where security responsibilities lie between us and our suppliers.

Security objectives

1. We seek to continually understand our appetite for balancing risks against opportunities.
2. We ensure we identify our assets and understand which are most important to us and those we serve.
3. We understand how our organisation and assets could be targeted.
4. We understand the Māori data we hold, and Treaty partners' security expectations.
5. We understand how our supply chains and relationships affect our security posture.

Prevent & Protect

We focus on reducing actual risk and seeking to frequently, incrementally improve our cyber security posture. Assets need protection in a way that prevents bad things from happening, and potential vulnerabilities are removed before they are exploited.

Security objectives

1. We build security and privacy into systems and services by default, enabling only the functionality that we need to meet our organisations outcomes.
2. We separate our systems so we can choose who is given access to each one.
3. We keep our systems up to date and use modern security features to protect our services.
4. We protect Māori data in line with Treaty partners' expectations.
5. Our users can be confident the system protects them from harm.

Detect & Contain

Incidents will occur and they need to be contained. Security monitoring is a necessary component of knowing when abnormal activity is occurring. Knowing how and why our systems interconnect is essential to limiting any potential spread.

Security objectives

1. We can tell when our systems are not operating normally.
2. We continuously check that our security controls are effective.
3. We minimise and monitor the interaction between our separate systems.
4. We control all the ways information can move off our systems.
5. We are able to isolate or contain systems when required.

Respond & Recover

We prioritise our security incident response to get critical services back to normal operation as fast as possible.

Security objectives

1. We focus on likely events, not worst-case scenarios.
2. Our response plans are flexible and can adapt as we gather better information.
3. We know who we can get help from before an incident happens.
4. We know our critical services and plan to get them back running first.
5. We practice our response plans to improve them and have confidence they will work.

How does the NCSC framework compare to NIST's cyber security framework?

Our framework is very similar to the NIST cyber security framework, and both contain five high-level functions. In our view, the main point of difference is that we have chosen to place greater emphasis on security governance and culture by separating it from the Identify function. To reflect the interconnected nature of incident response and recovery, we have merged NIST's Respond and Recover functions (which are separated in NIST's framework).

Figure 2: NCSC framework functions compared with NIST CSF functions.

We are adapting the NIST framework in two significant ways. Firstly, where the NIST framework details 22 categories and more than 100 sub-categories of activities under its five top-level functions, our framework focusses on describing what good outcomes look like for each of these top-level functions, rather than delving into the detail of each one.

Our view is that this will allow us to use the framework easily when engaging with other agencies who use different frameworks. It will also make it easier for us to organise, and demonstrate how cyber security activities such as the NIST CSF categories, ISO 27000-series domains, and the NZISM chapters can be organised under our framework.

The second adaption is our separation of the 'Guide & Govern' function - the NIST framework generally covers this as part of 'Identify'. Our aim here is to keep a distinction between cyber security governance activities and cyber security management; in our view, these are separate functions, often performed by separate parts of the business.

What next for our cyber security framework?

We have developed and refined our framework. Now that we have released a beta version of the framework, what is next?

Using the framework to help executives and senior leaders understand cyber security expectations

Cyber security is used to manage complex, organisation-spanning areas of risk. We plan on using the framework to shape and guide how we engage with leaders.

Identifying an appropriate maturity model for the framework

We received feedback that the framework would benefit from having a maturity model, but that agencies do not want an additional cyber security maturity model to grapple with.

At the NCSC, we are working on a cyber assessment and insights tool that is designed to help nationally significant organisations understand their cyber maturity. We will seek to integrate our framework with this tool as we develop it further.

Better integration of cyber security concepts with te ao Māori

As security professionals, we recognise that our industry has diversity challenges, which include a lack of Māori working in security, and a lack of Māori concepts and ways of thinking about outcomes in our tools and frameworks.

At the NCSC, we are working on how we encapsulate te ao Māori and engage Mātauranga Māori concepts when we think about cyber security in the public service.

Setting out how our framework maps to other frameworks

We plan on setting out how the framework can be used with:

- NZISM: we will do this through tagging the controls of the NZISM to each function
- NIST categories
- ISO27000-series domains.

The NCSC can be contacted by email at: **info@ncsc.govt.nz**
We encourage you to contact us at any time if you require any further assistance or advice.