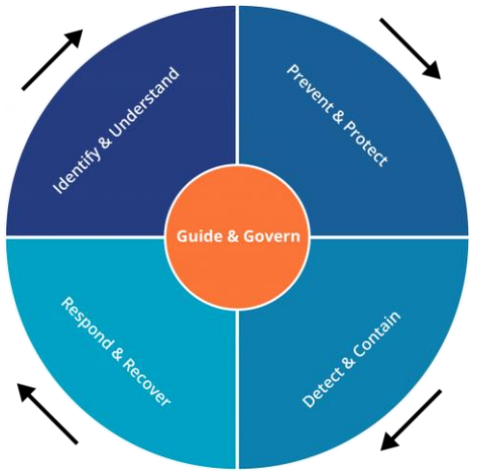
// NCSC Cyber Security Framework



The National Cyber Security Centre's Cyber Security Framework is a way of organising thinking about cyber security activities, and it provides a common language to describe them. Organisations can refer to the framework to understand how the NCSC uses advice, guidance, standards, and security services to communicate consistently what being *cyber secure* and *cyber resilient* means.

The National Cyber Security Centre (NCSC) has based its framework on the popular NIST Cyber Security Framework (CSF) and adapted this to the New Zealand context. The NCSC's framework content is freely available (under Creative Commons) for others to adopt or adapt to suit their own needs.

	Description	Objectives	
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.	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, and understanding the context and threat environment we operate in.	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.	1. We build security and privacy into systems and services by default, enabling only the functionality that we need to meet our organisation's 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.	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.	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 to normal first. 5. We practise our response plans to improve them and have confidence they will work.