Te Kāwanatanga o Aotearoa
New Zealand Government

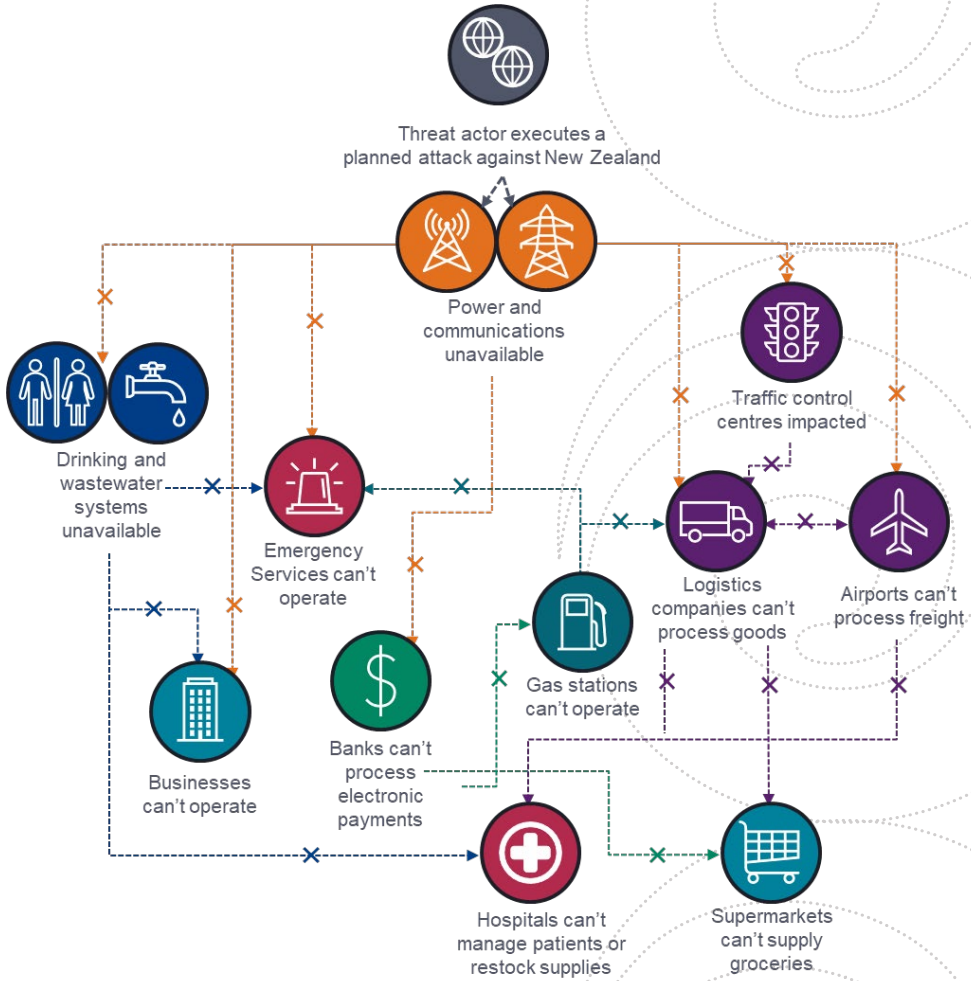
Enhancing the cyber security of New Zealand's critical infrastructure system

Digitally resilient critical infrastructure services to power New Zealand's economy and protect our communities

For Consultation – Not Government Policy

Current state of play

- The consequences of disruption can be significant
- Cyber threats are escalating
- There is no common baseline of cyber security across the critical infrastructure system
- We are not observing actions that match the level of cyber risk across the critical infrastructure system.



Two key questions

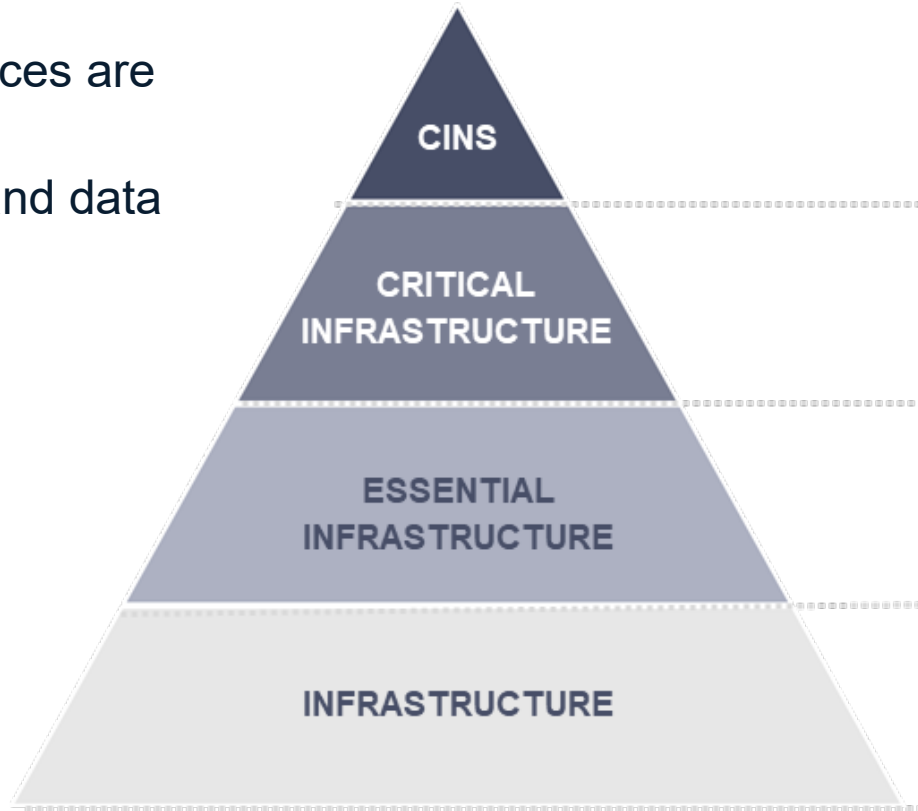
What are the infrastructure services most critical to our economy and communities that they should be safeguarded against harm?

What should the depth of the cyber defences of these infrastructure services be?

Defining critical infrastructure

Seven essential services are proposed initially:

- Communications and data
- Defence
- Energy
- Finance
- Health
- Transport
- Water



Critical infrastructure of national significance: the components providing essential services that, if disrupted, would have severely debilitating national consequences. e.g. core components for the operation of the national grid.

Critical infrastructure: the components providing essential services that, if disrupted, would have national or otherwise significant and/or widespread consequences, e.g. electricity generation over 30MW in aggregate.

Essential infrastructure: the components providing **essential services** that are necessary for public order, public safety, public health, national security or the functioning of the economy or society of the whole or part of New Zealand, e.g. electricity generation, transmission and distribution.

Infrastructure includes networks that provide services like communications, energy, transport and water and social infrastructure like education and research facilities, justice precincts and community facilities like parks and stadiums.

- Critical Components: the components that are necessary to the delivery of the relevant essential service, as determined by a reasonable person in the same set of circumstances
- Components: assets, information, networks, systems, suppliers, people and processes

Te Kāwanatanga o Aotearoa
New Zealand Government

Measures to enhance the cyber security of our critical infrastructure system

For Consultation – Not Government Policy

Improve information flows between critical infrastructure and government

Information flows to government
- Operations, including critical components
- Ownership and control
- Dependencies and interdependencies

Voluntary information exchange
- Critical infrastructure entities and government
- Information on risks and mitigations

Information flows between critical infrastructure entities
- e.g. restoration times

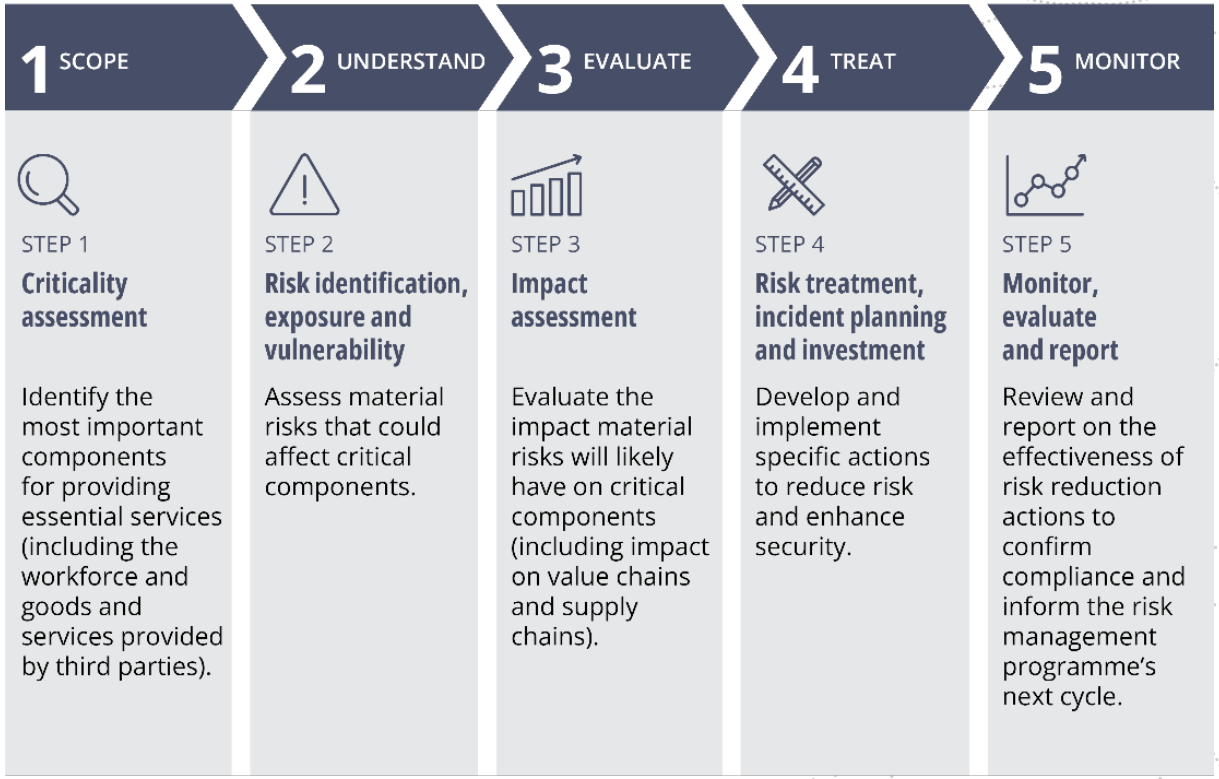
Information on cyber incidents
- Report all cyber incidents regularly
- Report all significant cyber incidents as soon as practicable

Information could only be…
- **used consistent with the purpose** of critical infrastructure security or preserving national security or public order.
- **shared with specified government agencies** that have a role in ensuring the security and ongoing operation of the critical infrastructure system.
- **disclosed to other organisations** if necessary preserve national security or public order.

Set minimum cyber risk management requirements

- Identify **components that are critical** to the delivery of essential services
- Identify **cyber risks that are material** to critical components
- **Treat material cyber risks to critical components** as far as reasonably practicable
- Align with an international cyber security framework

Directors responsible for meeting minimum requirements



A power to direct the management of cyber threats for national security reasons

Only when…

- the national security threat is significant
- adequate and good-faith consultation with the relevant entity(ies) has occurred
- the proposed action is proportionate, necessary and has a reasonable likelihood of success
- there is no alternative to the proposed action.

Could include requiring a critical infrastructure entity to accept support from the NCSC to help resolve cyber incidents that are a threat to national security.

Ensuring and new requirements enhance cyber security

Compliance toolbox would include:

- compliance notices
- legally binding agreements
- non-criminal monetary penalties
- criminal prosecution

Compliance would be staged and have an initial focus on providing information and guidance

CATEGORY OF BREACH	EXAMPLE COMPLIANCE TOOLS
Minor breach	• Targeted education. • Written warning. • Increased monitoring assessments. • Administrative fine of up to $50,000.
Minor to moderate breach	• Compliance notice or enforceable undertaking. • Increased monitoring assessment. • Information request or inspection. • Civil pecuniary penalty of up to $100,000.
Moderate breach	• Compliance notice or enforceable undertaking. • Civil pecuniary penalty of up to $200,000.
Serious breach	• Compliance notice or enforceable undertaking. • Criminal penalty of up to $2 million or up to 1 percent of annual turnover, whichever is greater (for an entity). • Criminal penalty up to $100,000 (for a director).
Critical breach	• Compliance notice or enforceable undertaking. • Criminal penalty of up to $5 million or up to 2 percent of annual turnover, whichever is greater (for an entity). • Criminal penalty up to $500,000 (for a director).

We need your feedback

Consultation closes 11.59pm 19 April

- Definitions and thresholds for critical infrastructure?
- Measures to enhance cyber security?
- The costs of enhancing cyber security?

Wellington	19 March	7:30-9am
Online	20 March	12-1:30pm
Auckland	23 March	7:30-9am
Hamilton	24 March	12-1:30pm
Christchurch	25 March	7:30-9am
Queenstown	26 March	12-1:30pm
Dunedin	27 March	12-1:30pm
Online	30 March	12-1:30pm

https://www.dpmc.govt.nz/our-programmes/national-security/critical-infrastructure

THANK YOU

criticalinfrastructure@dpmc.govt.nz

www.dpmc.govt.nz/our-programmes/national-security/critical-infrastructure