
GET in SHAPE
WEBINAR SERIES

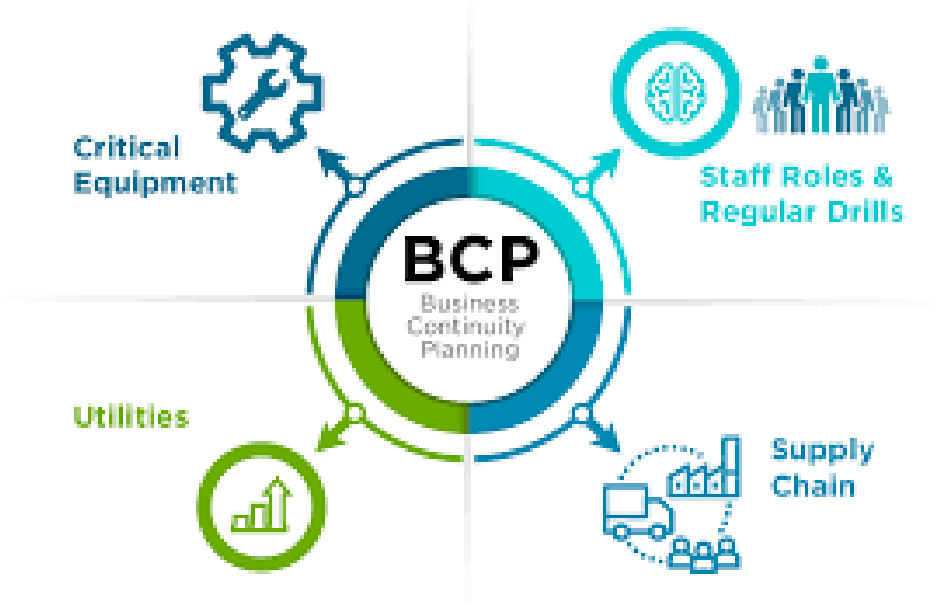
GET in SHAPE

WEBINAR SERIES

Business Continuity Plans and Cyber Security

Karty Mayne – Rosewill Consulting
Jeremy Muir - MinterEllisonRuddWatts

27 August 2021



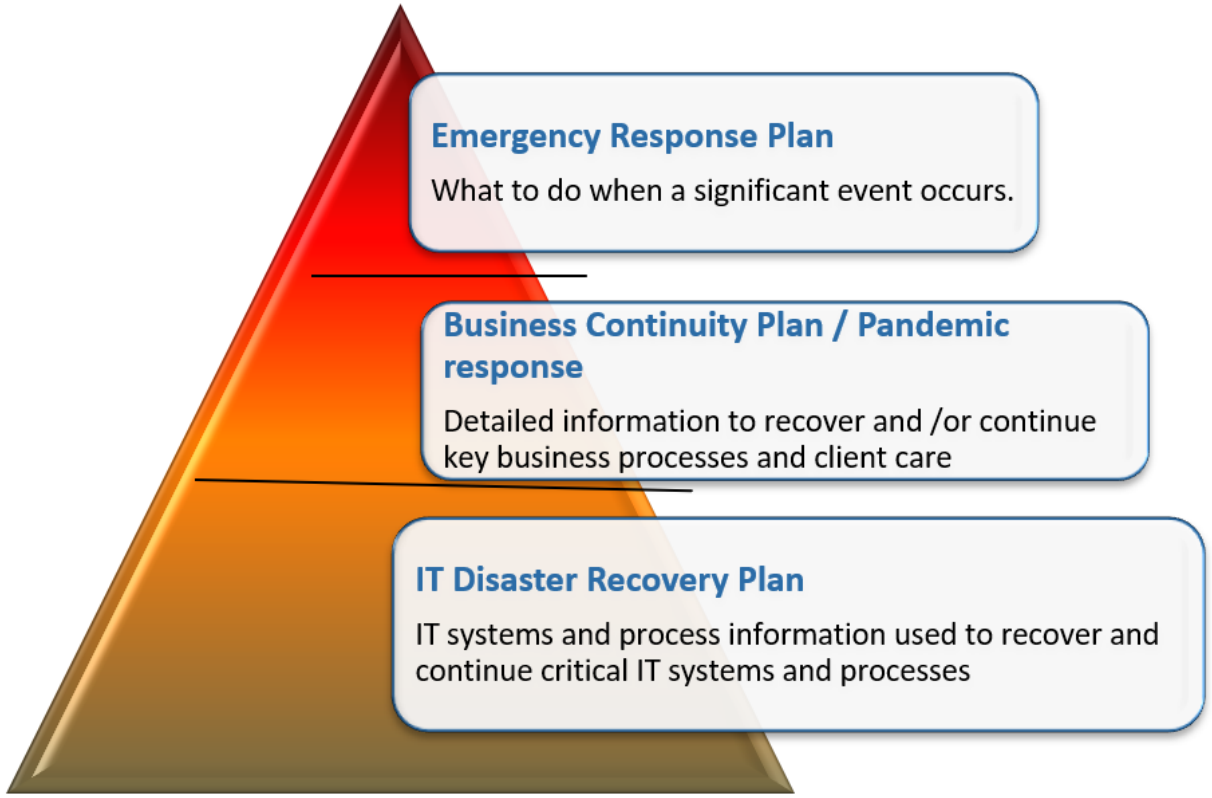
Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

The importance of being able to run your business safely and remotely

- Covid lockdowns make for a great BCP test!
- Cyber security will be high on your key business risks
- What is the latest guidance on cyber security from the FMA?
- How do you evidence testing your BCP?

What is a BCP?



Business continuity starts with keeping people safe.

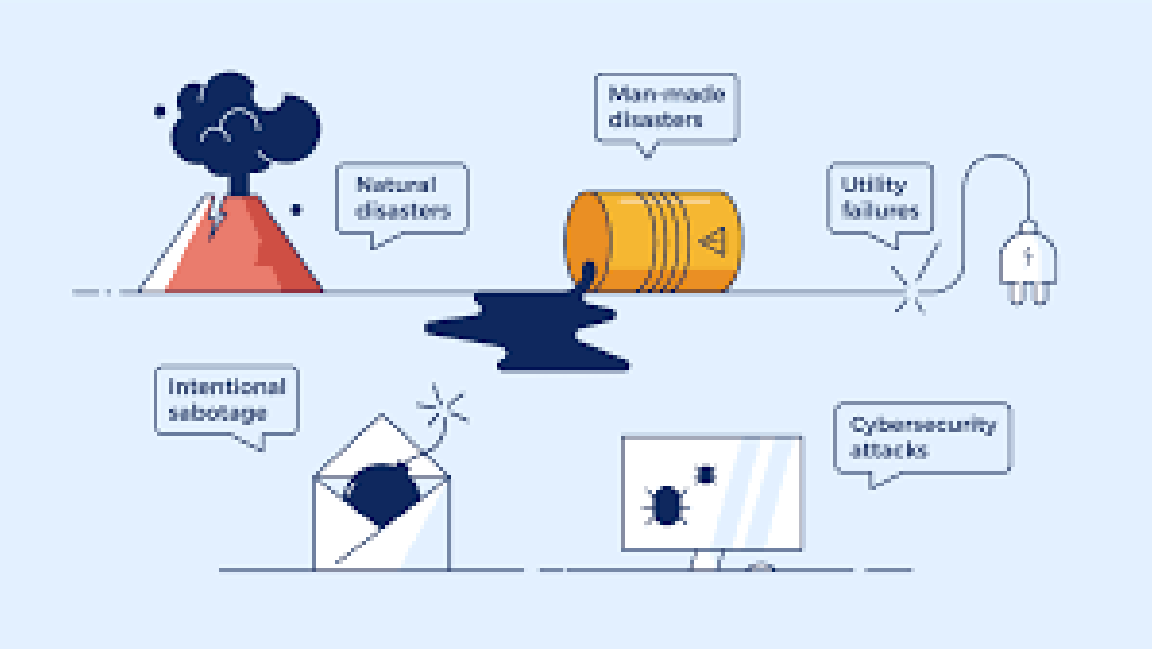
There are three key elements to business continuity planning:

1. Emergency response
2. Business continuity
3. Disaster recovery

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Where are the business risks?



There are numerous scenarios that may disrupt your business.

Common scenarios include:

a. loss of key staff (temporary or permanent staff);
b. loss of building;
c. denial of access to building for a limited time;
d. loss of IT (data);
e. loss of IT (voice);
f. loss of vital (non-electronic) records; and
g. loss of key dependencies.

The impact may be minor, severe or critical, depending on the incident.

Purpose of Business Continuity planning

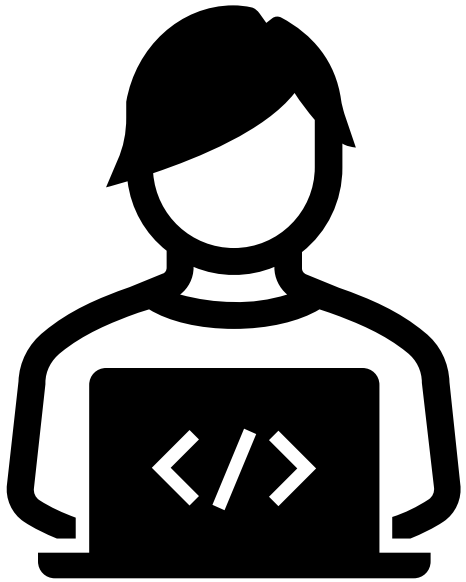
1. Make it easy to run your business from afar
2. Identify possible events (natural disaster, cyber security breach, viral outbreak, power loss etc)
3. Assess critical business functions.
4. Identify back up strategies and alternative locations, functions and people.
5. Document possible responses and options.
6. Create quick reference contact lists, checklists and reference notes.

What should your BCP contain?

A BCP is a detailed plan outlining the actions to take in the event of a disruption to the FAP's business, to ensure it can continue to operate.

This plan may include the following:

- ✓ The steps to restore operations – who does what, where to relocate to and how.
- ✓ Identification of critical systems.
- ✓ List of vendors that should be notified of the disruption.
- ✓ Copies of licenses and contracts held with third parties detailing maintenance and support.
- ✓ The process to contact and advise clients of any loss of service.
- ✓ The process for providing an alternative service to clients during any downtime. This may include provision of a 'locum' to act on your behalf by prior arrangement.



Locum arrangements

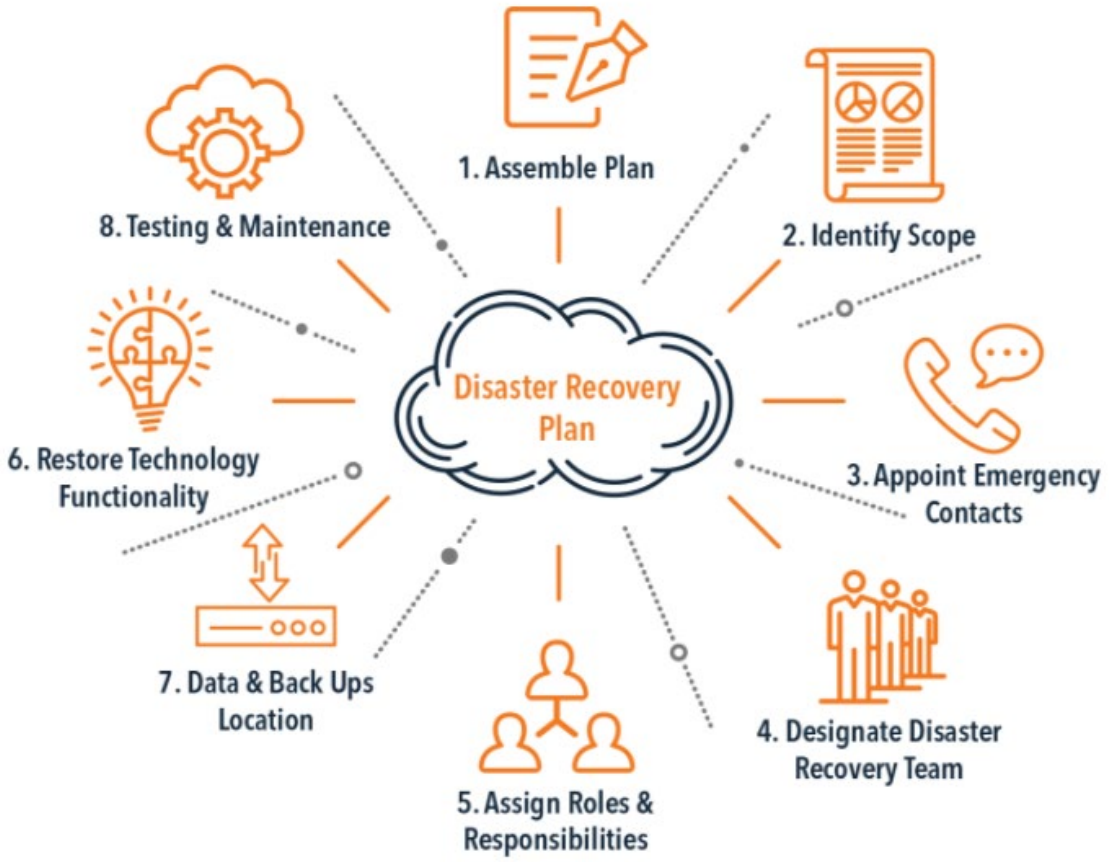
- How you will provide an alternate service to clients during any downtime. This might include a provision of a “locum” to act on the FAP’s behalf.
- Create a written agreement setting out delegated authority and your agreed arrangements.

Areas to consider:

- Remuneration
- Systems
- Access
- Log in
- Priorities
- Initiating your locum
- Extended periods
- Capacity and capability

GET in SHAPE

Purpose of Disaster Recovery Planning



1. Can a non IT person recover your data?
2. Key focus is on recovery of your IT and business systems.
3. Need to recover and protect client information.
4. Set recovery time objectives.

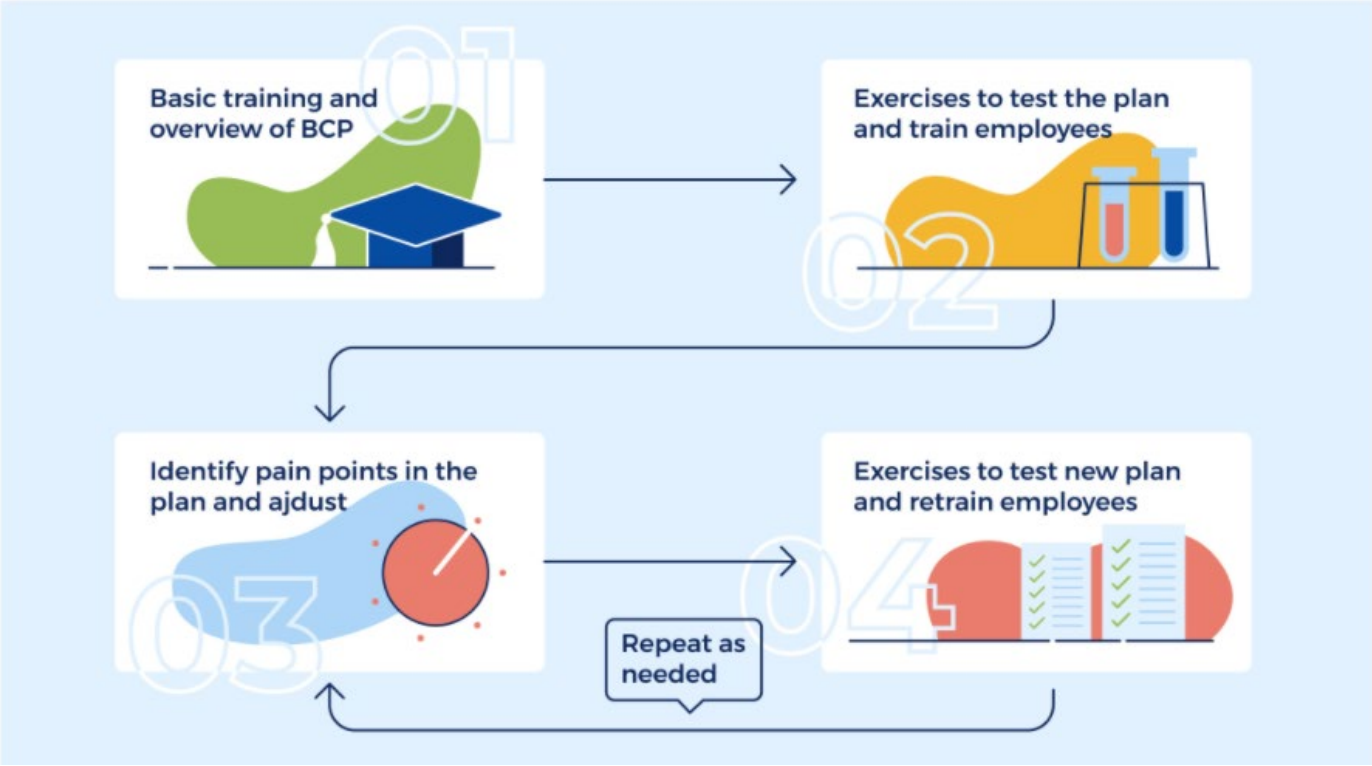
Writing Your BCP – 3 Easy Steps

1. Start with a good template.
2. Get everyone in your business involved in risk assessment and planning.
3. Assign a BCP owner to keep it up to date.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

4 easy steps to an effective BCP



1. Provide your team with an overview of your BCP and basic training
2. Run tests or exercises to get everyone trained
3. Iron out any pain points
4. Keep testing, training, adjusting

Rinse and Repeat!

Hint: real events can count as a BCP test.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Easy ways to record your BCP tests

BCP Tests	Date of Test	Test Notes and Comments: Issues, Changes, Purchases	Date of next test	Sign off
Test to ensure we can make contact in an emergency				
Test that we can function at alternative premises				
Test that we can restore our systems				
Test to ensure file recovery.				
Test to confirm procedures to follow in the event of a cyber security attack.				

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

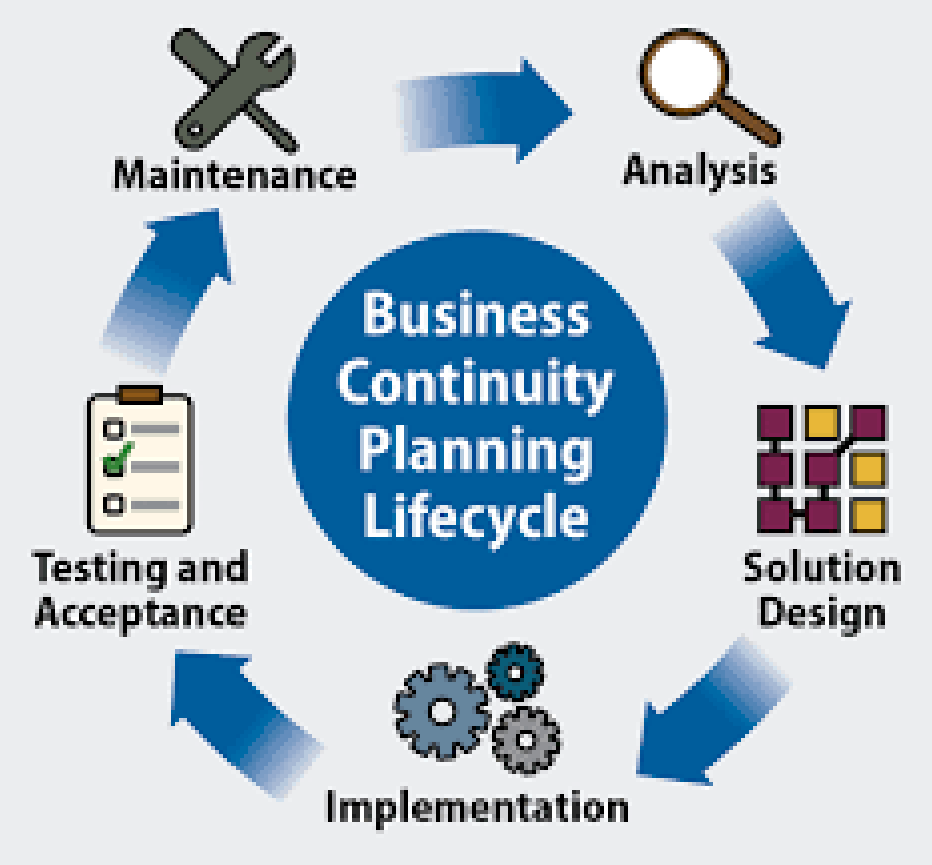
Keep your BCP current

Internal or External reviews
Conduct a review of your plan at least annually.

Updates will be required due to:

- Threats to the environment
- Exercises that indicate the need for change
- Changes to company structure or personnel
- Geographic distribution of employees

Summary



1. Your BCP needs a continuous life cycle
2. Schedule time for ongoing training
3. Use mock scenarios to iron out the kinks
4. Very important to keep your BCP up to date.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

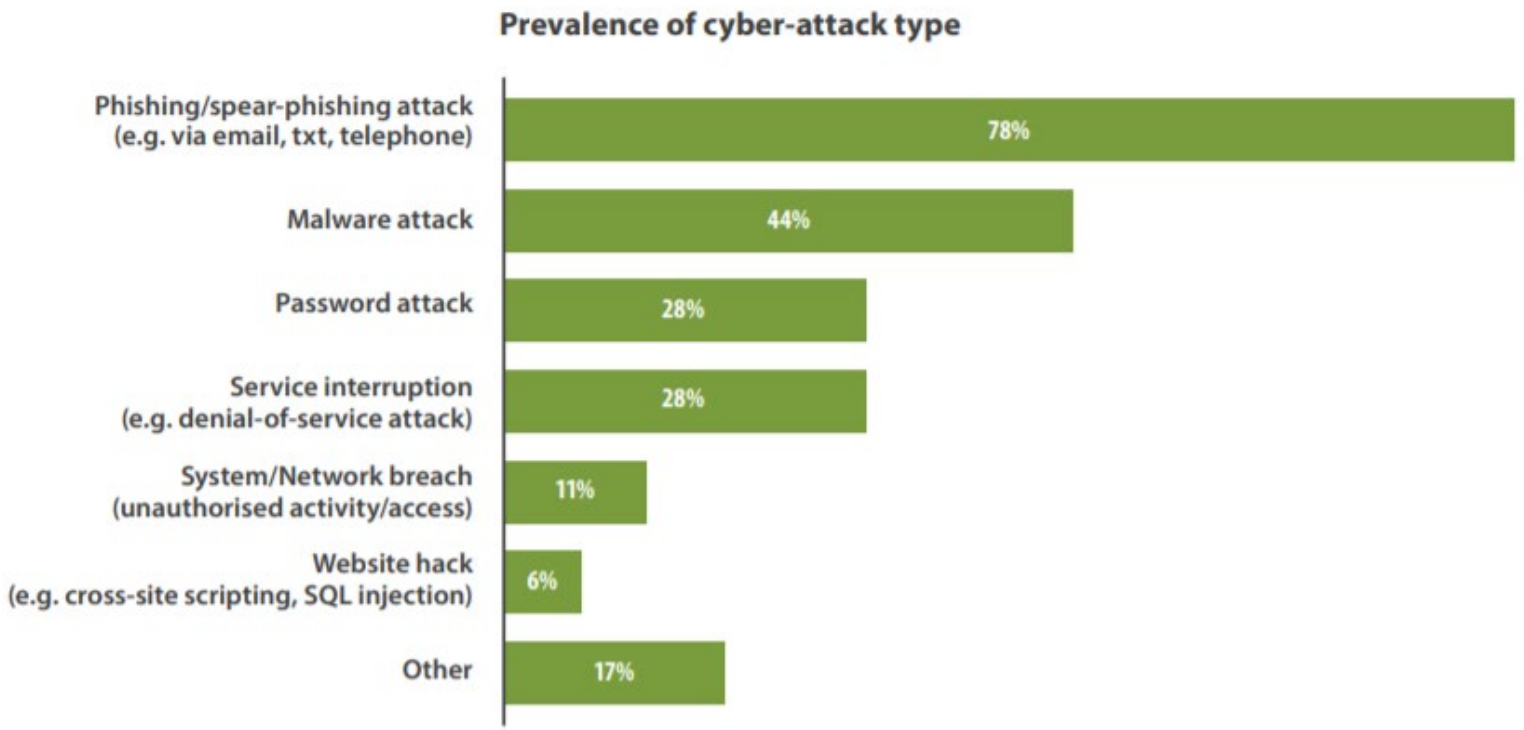
Cyber Security Basics

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Cyber Attacks in New Zealand

Source: Financial Markets Authority | Cyber-resilience in financial services July 2019



Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Your Obligation – Protect Client Information

Standard 5 – Protect Client Information

Code of Professional Conduct for Financial Advice Services

Requires you to:

- protect client information against loss and unauthorised access, use, modification, or disclosure.

This requires you to address your cyber-security.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Your Regulatory Obligations

Standard Condition 5 states:

- If you use any technology systems, which if disrupted would materially affect the continued provision of your financial advice service (or any other market services licensee obligation), you must at all times ensure that information security for those systems – being the preservation of confidentiality, integrity and availability of information and/or information systems – is maintained.
- You must notify the FMA within 10 working days of you discovering any event that materially impacts the information security of your critical technology systems and provide details of the event, the impact on your financial advice service and clients, as well as your remediation activity.
- Note that your business continuity plan must have predetermined procedures for responding to, and recovering from, events that impact on your cybersecurity.

Does you have an approved documented cybersecurity policy?

This includes having adequate and effective IT systems to:

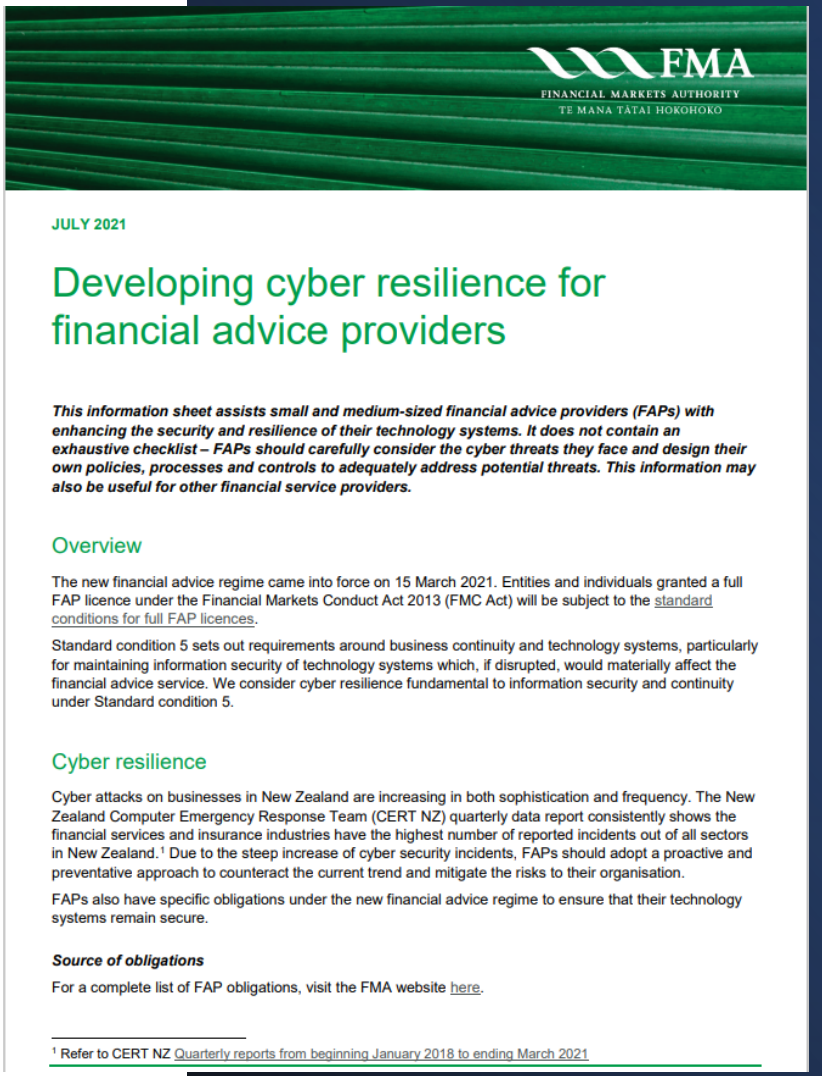
- maintain cyber-resilience to detect, prevent and respond to cyber-risks
- maintain client records
- protect client data and confidential information.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Develop your cyber resilience:

- Use services provided by CERT NZ and New Zealand's National Cyber Security Centre.
- Assess cyber risks as part of wider risk assessment and management programmes.
- Use a recognised cybersecurity framework to assist with planning, prioritising and managing cyber resilience (for example the National Institute of Standards and Technology (NIST) cybersecurity framework core).
- Have an appropriate balance between protection and detection measures, avoiding over-reliance on protection measures alone.
- Governance arrangements must include board and/or senior management ownership and visibility of the cyber resilience framework.



FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

JULY 2021

Developing cyber resilience for financial advice providers

This information sheet assists small and medium-sized financial advice providers (FAPs) with enhancing the security and resilience of their technology systems. It does not contain an exhaustive checklist – FAPs should carefully consider the cyber threats they face and design their own policies, processes and controls to adequately address potential threats. This information may also be useful for other financial service providers.

Overview

The new financial advice regime came into force on 15 March 2021. Entities and individuals granted a full FAP licence under the Financial Markets Conduct Act 2013 (FMC Act) will be subject to the standard conditions for full FAP licences.

Standard condition 5 sets out requirements around business continuity and technology systems, particularly for maintaining information security of technology systems which, if disrupted, would materially affect the financial advice service. We consider cyber resilience fundamental to information security and continuity under Standard condition 5.

Cyber resilience

Cyber attacks on businesses in New Zealand are increasing in both sophistication and frequency. The New Zealand Computer Emergency Response Team (CERT NZ) quarterly data report consistently shows the financial services and insurance industries have the highest number of reported incidents out of all sectors in New Zealand.[1] Due to the steep increase of cyber security incidents, FAPs should adopt a proactive and preventative approach to counteract the current trend and mitigate the risks to their organisation.

FAPs also have specific obligations under the new financial advice regime to ensure that their technology systems remain secure.

Source of obligations

For a complete list of FAP obligations, visit the FMA website here.

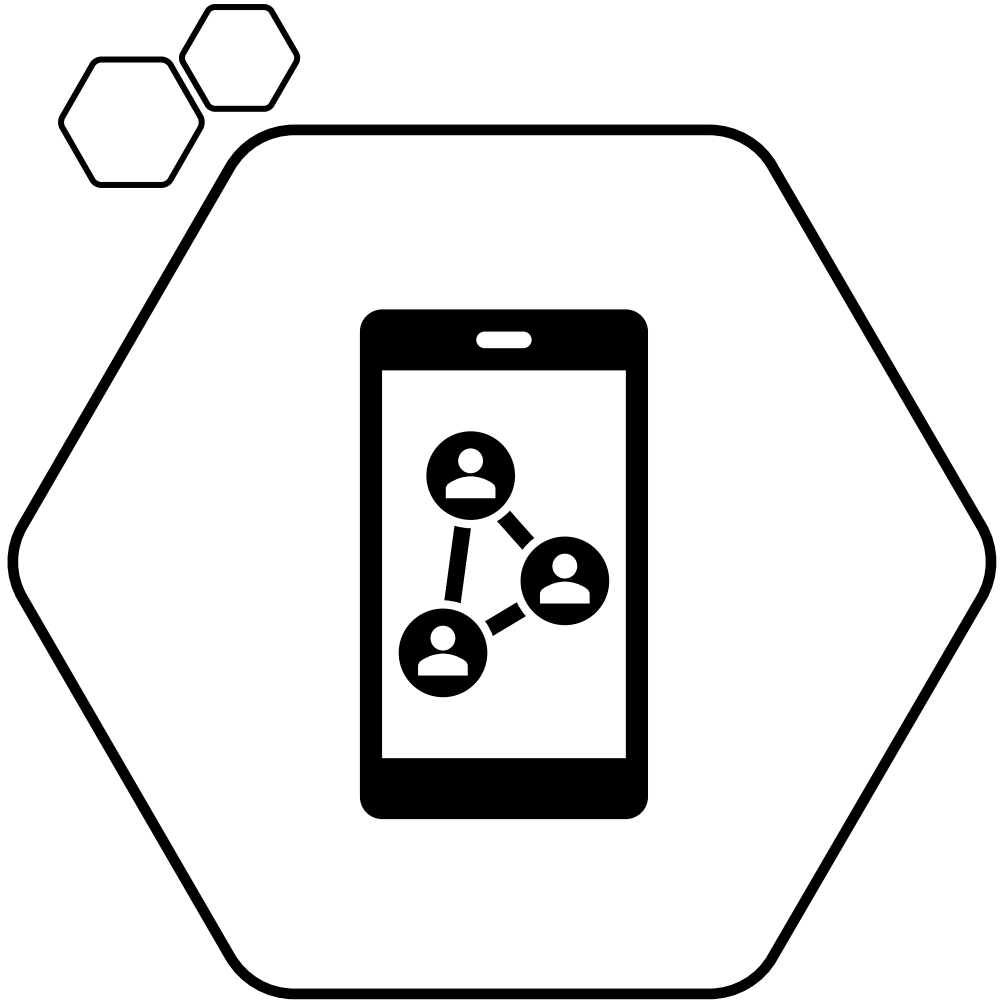
[1] Refer to CERT NZ Quarterly reports from beginning January 2018 to ending March 2021

Financial Services Council.
Growing and protecting the wealth of New Zealanders

Top Tips

CERT NZ and the National Cyber Security Centre

1. Back up your data
2. Keep your devices and your apps up-to-date
3. Choose unique passwords
4. Turn on two-factor authentication
5. Be creative with the answers to your account recovery questions
6. Avoid sensitive transactions on free Wi-Fi
7. Install an antivirus and scan for viruses regularly
8. Be smart about social media
9. Limit the personal information you give out online
10. Check your bank statements



Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Thank You

Karty Mayne

Rosewill Consulting

T: +64 274 666 686

karty@rosewillconsulting.co.nz

Jeremy Muir

MinterEllisonWattsRudd

T: +64 9 353 9819

Jeremy.Muir@minterellison.co.nz

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE

Next Webinar

Get In Shape Webinar Series: Session 20

Financial management and commercial considerations for the new regime with David Greenslade and David Ireland

9.30am, Friday 22 October 2021

Registration details can be found on the FSC Website under 'Events' and will also be sent via FSC emails.

Contact fsc@fsc.org.nz to subscribe.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

GET in SHAPE