FINANCIAL ADVICE NZ WEBINAR SERIES

THE ROAD AHEAD

Enhancing your Business Continuity Plan

Agenda

- Standard Condition 5 for FAP Licences
- The Code
- What's working well – BCP testing from our panel
- Cyber security - policy -processes
- Cyber issue case study example
- Tools and resources

Financial Advice NEW ZEALAND

Standard Condition 5 for FAP Licences

Business Continuity & Technology Systems

- You must have and maintain an up-to-date business continuity plan that's appropriate for the scale and scope of your financial advice service business.

- If you use any technology systems that are critical to the provision of financial advice service, you must ensure the information security of those systems is maintained.

- You must notify FMA within 10 working days of discovering any material information security breach.

The Code – Standard 5

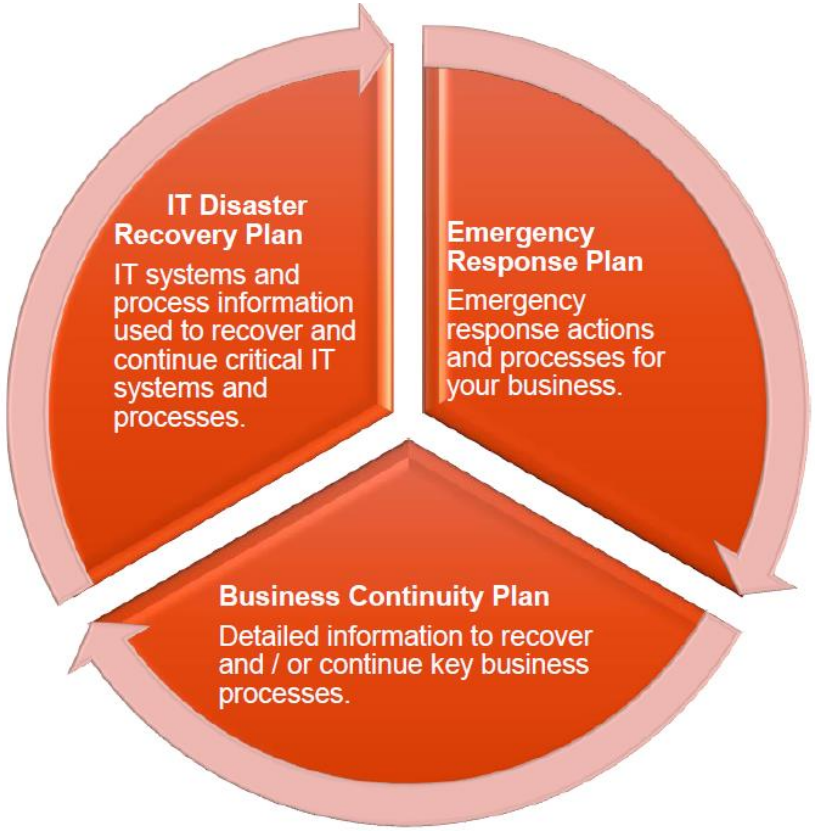
Protect Client Information

- You must take reasonable steps to protect client information against loss and unauthorised access, use, modification or disclosure.

Financial Advice NEW ZEALAND

Components of an effective BCP

The key components of a BCP are illustrated in the diagram showing the relationship of the Emergency Response Plan (**ERP**) Business Continuity Plan (**BCP**) and the Technology Disaster Recovery Plan (**DRP**).



Financial Advice NEW ZEALAND

BCP tips with our Panel

Let’s talk about how you :

- Respond
- Recover
- Resume and
- Restore

the level of operation following a disruption to business.

Financial Advice NEW ZEALAND

Cyber Security – what's your policy?

- Let's talk about what you have in place
- Have you tested this?
- Any issues or threats made to your data?
- What happens if there is an issue?
- How your Cyber security policy & support team can help you out.
- Example of a recent case.

Financial Advice NEW ZEALAND

Cyber Security – what's your policy?

Examples:

- Install software updates when available
- Implement 2 factor authentication
- Back up your data
- Set up logs
- Create your plan (BCP)
- Secure your devices
- Secure your network
- **Test your plan at least annually**

How are you recording your test?

Example BCP Tests	Date of Test	Comments	Sign Off	Next test date
Test to ensure we can contact all staff in an emergency	15/2/2021	all records up to date.	LH	15/02/23
Test that we can function at alternative premises	15/2/2021	Tested several times during lockdowns of 2020 and 2021. Also tested in February 1999 when the roof of our office block collapsed and we were not allowed onsite. All client files were able to be accessed, clients received seamless service, used alternative site (HB Business Hub) and technology (zoom). Access to client files was seamless, just needed to set up a printer driver to print documents at the Business Hub.	LH	15/02/23
Test that we can restore our systems	15/2/2021	Outsourced to our Tech Service Manager – test completed and logged	LH	15/02/23
Test we can access technology, access to files and working from alternative premises	Jan/Feb 2023, HB Business Hub closed and moving so no access to building or office	Client files and access to technology seamless. Alternative premises offered at client homes/offices and using technology (zoom). Very smooth and had no issues. Good result.	LH	15/02/23

Reference material and tools

- CERT NZ – https://www.cert.govt.nz/
- FMA self assessment tool – cyber security and BCP
- FMA guide – developing cyber resilience for FAP's
- Financial Advice NZ – BCP & Technology workbook

Financial Advice NEW ZEALAND

Summary - key points

- **Regularly identifying and reviewing risks and cyber threats**
- Implementing measures that **maintain the level of information security necessary for your FAP.**
- Having effective processes that monitor and detect activity that impacts information security
- Including in the business continuity plan the predetermined procedures for responding to, and recovering from, events that impact information security.
- Regularly test systems and controls