Full Licensing Standard Condition

Business continuity and technology systems

This Workbook is one in a series of workbooks to assist Financial Advice New Zealand members meet their obligations and standard conditions under full licensing requirements.

Version 2 - June 2021

Financial Advice NEW ZEALAND

TABLE OF CONTENTS

WORKBOOK OVERVIEW

We have created this Workbook for our members to use as a guide to help prepare for full licensing conditions as explained in detail on the page below.

If you are granted a full financial advice provider (FAP) licence by the FMA, the licence will be subject to conditions. See section 402 of the Financial Markets Conduct Act 2013 (**FMC Act**).

Your licence application will include details of your FAP business and details of how you will comply with:

- Financial Markets Conduct Act 2013 (FMC Act)
- Financial Markets Conduct Regulations 2014 (FMC Regulations)
- Code of Professional Conduct for Financial Advice Services
- **Conditions** imposed by the FMA (standard conditions)
- Or **specific conditions** applied by the FMA.

Conditions will include:

- a condition that the licensee or authorised body may, under the licence, only provide the market services or class of market services to which the licence relates and for which each person is authorised under the licence (see section 402(1)(a) of the FMC Act)
- conditions imposed by the FMA under section 403 of the FMC Act – these will generally include: the **standard conditions** and any **specific conditions** any conditions imposed by regulations.
- as at November 2020 the relevant regulations are the Financial Markets Conduct Regulations 2014 (the **FMC Regulations**)

Standard conditions

Where we refer to full FAP licence standard conditions, this means the following conditions which will be effective on and from 15 March 2021:

1. Record keeping
2. Internal complaints process
3. Regulatory returns
4. Outsourcing
5. **Business continuity and technology systems**
6. Ongoing requirements
7. Notification of material changes

STRUCTURE OF THIS WORKBOOK

This Workbook is part of a series of workbooks. Each workbook will deal with one Standard Condition for full financial advice providers licences. There are seven Standard Conditions in total.

Section A – Standard Condition

Provides the actual wording of your obligations with commentary from the Financial Markets Authority (FMA).

Section B – Examples of policies, processes, and controls

Provides examples of actions that evidence your obligations, with examples of practical policies, procedures and controls.

Section C – Supporting tools and checklists

For the business continuity and technology standard condition we have put together a checklist to assist you to prepare a business continuity plan.

SECTION A – STANDARD LICENSING CONDITION 5
BUSINESS CONTINUITY AND TECHNOLOGY SYSTEMS

Condition:

You must have and maintain a business continuity plan that is appropriate for the scale and scope of your financial advice service.

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 us 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.

Explanatory note from the FMA:

Your *business continuity plan* includes the documented procedures that guide you to respond, recover, resume and restore a pre-defined level of operation following disruption. This plan should provide for the continuity of your financial advice service generally – not just the recovery of your technology systems. It should also encompass any outsource arrangements, such as your client data provider.

Your plan should consider the loss of availability of your key resources, including staff, records, systems, suppliers and premises. The extent of your business continuity plan should reflect the size and complexity of your financial advice service, operational arrangements and exposure to disruptive events. A small business with simple processes and technology may only need a relatively brief plan covering a more limited range of likely disruptive events, but the plan is more likely to include locum arrangements.

A larger or more complex business, relying more extensively on technology systems and possibly operating from multiple locations will need to consider a wider range of disruptive events and reflect this in a more comprehensive business continuity plan.

Irrespective of the complexity of your circumstances, it is important that your business continuity plan is maintained, reviewed and regularly tested – at least annually. Your business continuity plan must also be updated immediately if there is a material change in business location, structure or operations.

Critical technology is that which supports any activity, function, process, or service, the loss of which would materially affect the continued provision of your financial advice service or your ability to meet your licensee obligations.

This condition requires that you maintain the information security of your critical technology. This includes:

a) regularly identifying and reviewing your risks and cyber threats; and

b) implementing measures that maintain the level of information security necessary for your risk profile; and

c) having effective processes that monitor and detect activity that impacts your information security; and

d) including in your business continuity plan your predetermined procedures for responding to, and recovering from, events that impact on your information security.

The information security of your critical technology systems should be managed within the risk tolerance set through your governance processes. We recommend that you use an appropriate, recognised information security framework for this purpose.

You must have arrangements in place to notify us in the event of a material information security breach. A material event is one where the confidentiality, integrity or availability of your information and/or your technology systems has been compromised. You do not need to notify us of minor events, such as receiving a 'phishing' email.

SECTION B – EXAMPLES OF POLICIES, PROCESSES AND CONTROLS

Actions that demonstrate the standards have been applied.

The FMA may ask for evidence that you are meeting the standard conditions of your licence, therefore having robust policies, processes and controls will help you demonstrate you are meeting these requirements.

Evidence

1. Develop Business Policies
2. Develop Procedures – tasks
3. Develop Controls – checks

On this level you need to refer to your Business Policies, Procedures and Controls (PPCs).

It is very important that your PPCs are not too complex or complicated.

From the worked examples you will realise you already have many 'policies, procedures, and controls', but you may need to work on building, adapting, articulating and documenting these. An FMA review will likely be based on the evidence you supply, so it is vital your PPCs are documented and accessible.

1. BUSINESS CONTINUITY AND TECHNOLOGY SYSTEMS

Example of policies, processes, and controls.

1. Develop Policy statement

Our business can continue to operate in the event of a disruption and systems can be reactivated with critical functions restored within 24 hours of being interrupted, with all other systems up and running within 2 working days.

2. Develop Processes and Procedures (tasks)

- Create a Business Continuity Plan.
- Select a person to be responsible for the upkeep of the plan.
- Train all relevant people in your business on how the plan is activated and managed.
- Test the plan at least every 6 months or annually.

3. Develop Controls (check it is working)

BCP Testing

- Have the testing verified as part of your external compliance review or reviewed by a designated person in your FAP.

Checks should include:

- Whether the BCP was reviewed in the timeframe and manner as required and
- If all directors, financial adviser and support staff were briefed on their duties.

SECTION C – SUPPORTING TOOLS AND CHECKLISTS EXAMPLE

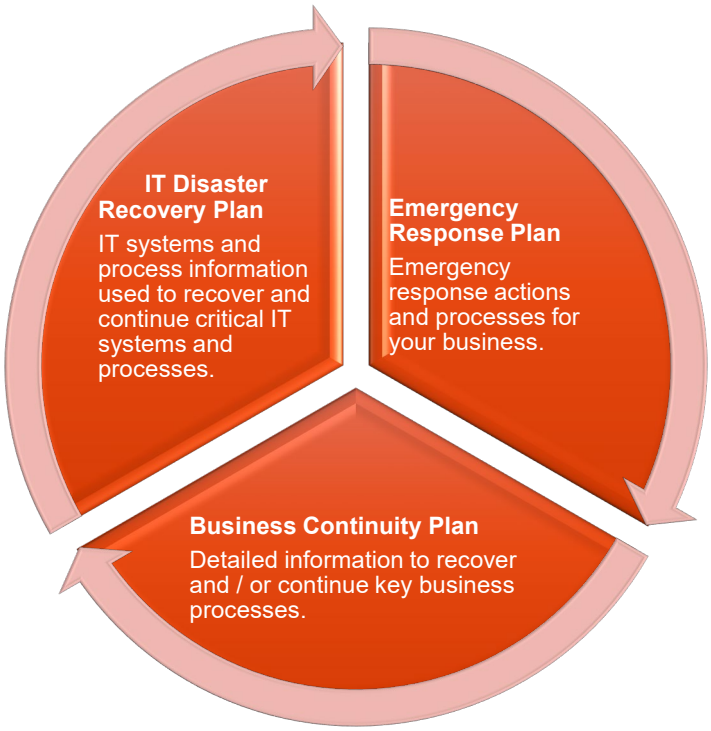
Introduction

A Business Continuity Plan (**BCP**) is the integrated plan and management processes applied when a business experiences an event which does or could impact on normal business activity and providing service to your clients.

You should identify, assess, manage, mitigate and report on potential business continuity risks as well as ensure the welfare of your people, clients and facilities in the event of a disruption. This is all relevant to the size and structure of your business so making these plans needs to be practical and easy to implement whether you are a solo practitioner or in a team of 20 or more.

Components of an effective BCP

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



EMERGENCY RESPONSE PLAN

In the event of an emergency

- Remain calm.
- Notify emergency services – dial 111.
- Follow the instructions of Building Wardens and/or Civil Defence where applicable.
- Take any action required to keep employees, clients, visitors and contractors safe from harm.
- Notify your Crisis Management Leader (if you have one).

Crisis Management

Appoint a Crisis Management Leader (**CML)**, if this is relevant to the size and structure of your business.

This is the person who has the responsibility for the overall management of the disruption.

The principle purpose of the CML in their emergency response is to **look out for people and property.**

CML Priorities

- Obtain information on the incident.
- Activate the appropriate response plan.
- Ensure the welfare of staff and clients.
- Provide leadership and direction in a crisis.
- Provide a decision making and communications channel.
- Seek specialist advice as required (e.g. Property management, technology events etc).

Crisis Management Leader Checklist

Incident Management	• Determine size of incident and level of response required. • Activate the BCP using text, phone or email. • Assign roles and responsibilities. • Document your response.
People	• Obtain assurance on staff safety. • Understand the immediate needs of staff during incident. • Check whether any clients or visitors are in the office. • Provide an information and communication channel for staff. • Decide on office(s) closure.
Premises	• Prioritise people's safety. • Determine impact on premises. • Secure premises. • Obtain assurance premises are safe before staff and client return. • Obtain structural engineering reports of affected premises if needed. • Arrange communication channels for information to staff and clients on premises.
Business Continuity (IT and DR)	• Advise on status of IT systems. • Enable telephone diversions (where necessary). • Enable remote access. • Identify critical functions and business continuity plans for critical functions. • Determine services affected. • Activate a Disaster Recovery Plan (if required).
Business Continuity (Client Servicing)	• Ensure client safety. • Ensure communication channels for clients (phone diversions etc). • Activate the BCP as required.
Business Continuity (Premises)	• Control access to premises (security passes to deny/allow access). • Work in partnership with landlords/building managers. • Notify security monitoring of premises status. • Co-ordinate repairs and structural engineers' inspections if needed. • Activate the BCP/DRP as required.

BUSINESS CONTINUITY PLAN CHECKLIST

Critical services and functions

In this area consider all core products or services and activities that you complete in your business. Following a significant business disruption list the critical business functions that must be completed.

1. **What are your critical services and functions**?
2. **Who completes** these services in the business?
3. **Who else** can do these?
4. Do you need a **locum Financial Adviser** in the event you cannot continue providing these services?

5. What do you consider to be **essential equipment?**

Premises

For consideration in the event premises were unable to be occupied for an extended period due to circumstances beyond the control of occupier (e.g. fire, earthquake etc)

6. What are your **relocation options**?
7. Location of another office to work from for a short, medium, or longer term?

People

8. Do you have the **current contact details** of everyone who works in your business?

Key Suppliers contacts

9. **Insurance providers - contact details**

10. **Equipment providers – contact details**

11. Utility providers – contact details

Plan, Prepare and Practise!

DISASTER RECOVERY PLAN

The Disaster Recovery Plan (DRP) explains procedures to recover technology and IT systems in the event of an emergency situation.

Objectives of our Disaster Recovery Plan:

- All staff understand their duties in implementing the documented plan.
- Our policies are adhered to.
- Ensure contingency arrangements are cost-effective; and
- Disaster recovery considers our customers, staff, suppliers, and others.

In the event of a crisis speedy decisions are often needed without all the information normally relied on. It is necessary for everyone to be aware of what needs to be in place to restore our business in the event of a crisis.

What to consider:

- Where the data may be stored and backed up. Is the location of the backup appropriate in the event of an emergency? Or is it cloud based and not impacted?
- If data needs to be reconstructed, consider who may have access to the records both internally and externally (employees, clients, suppliers, IRD etc). Ensure any reconstructed data is backed up.
- How would the reconstructed data be stored if required?
- Where is back up data stored and who has access? Would they know where to find and retrieve the information? Should the backed-up data be stored in the Cloud?
- Include in any back up client contact lists, process manuals and important contacts.
- Loss of essential services.
- Loss of key personnel.

IT Systems

Consider the following items when assessing your IT systems:

- Our current IT systems are XXXXX (CRM or key system you use to hold client information).
- Are they cloud based or server based?
- Back up data plan?
- Accessibility in an emergency is by XXXX.
- How do we continue to interact and service clients – Zoom, Google Hangout, Microsoft Teams, or other virtual means.

Systems Recovery

In the event of a system failure describe how to apply back-ups etc to enable quick recovery.

- System type - Method of backup and recovery – Location.

certnz

Protect your business online

Cyber security is more important than ever. There's a lot to consider when keeping your business secure like protecting your data, your network, and your customer information. Follow our top tips to help keep your business safe online.

/// Install software updates

Stop attackers getting access to your business network through known vulnerabilities, by regularly installing the latest software. Software updates often contain security fixes.

/// Implement two-factor authentication (2FA)

Make sure anyone who logs in to your system has to provide something else on top of their username and password, to verify that they are who they say they are.

/// Back up your data

Regularly back up your business data. Set your backups to happen automatically and store them somewhere secure offline. You can then restore your data if it's lost, leaked or stolen.

/// Set up logs

Logs record all the actions people take on your website or server. Set up alerts to notify you if an unusual event occurs. Make sure someone checks the logs when an alert comes in.

/// Create an incident response plan

An incident response plan will help you get your business back up and running quickly if your business is targeted by cyber attack. Talk to your staff about the plan ahead of time.

/// Change default passwords

Check for default passwords on any new hardware or software. If you find any default credentials, change the passwords for them.

/// Choose the right cloud services

Select a cloud services provider who will provide the right services for your business. Check their data and security policies. Ask if they'll do backups and if they offer 2FA.

/// Only collect the data you need

The more data you hold about your customers, the higher your security risk. This data is valuable to attackers so reduce your risk by only collecting what you need.

/// Secure your devices

Enable security software, like antivirus, to prevent malicious software being downloaded to any device that accesses your business data or systems.

/// Secure your network

Configure network devices like firewalls and web proxies to secure and control connections in and out of your business network. Use a VPN that uses 2FA if you need to remotely access systems on your network.

/// Check financial details manually

If you need to pay a new supplier, or to change bank details, double check it manually — by phone or text — before you approve any payments. Do this for any unusual or unexpected requests too.

To report a cyber security incident, visit **www.cert.govt.nz**

Top tips for cyber security

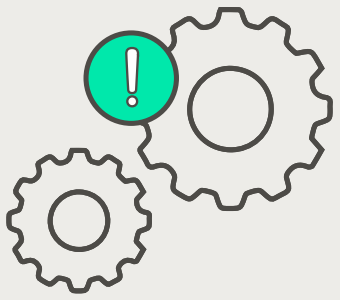
certnz

Online security is becoming more important than ever. While there's no bulletproof way to prevent a cyber attack, here are some easy tips to help you keep your personal information safe and secure.

Back up your data

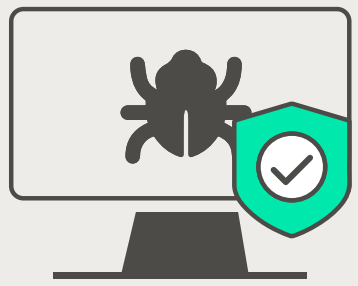
Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.

Keep your operating system up to date



Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.

Install antivirus software



Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.

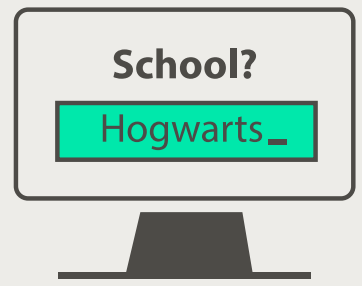
Choose unique passwords

Create unique passwords for each account – that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.

Set up two-factor authentication (2FA)

Choose to get a code sent to another device like your phone when logging in online – it helps stop hackers getting into your accounts.

Use creative recovery answers



Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.

Be cautious of free WiFi networks

Be careful using free Wifi and hot spots - they are untrusted networks so others could see what you are doing.

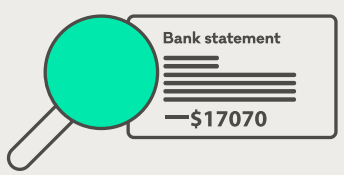
Be smart with social media

What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

Don't give out personal info

Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.

Check bank statements regularly



Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.

Get a regular credit check

An annual credit check will alert you if someone else is using your details to get loans or credit.

To report a cyber security problem, visit **www.cert.govt.nz**

The information provided in this workbook is for general information only and is not legal advice.

The source of information used in this Workbook is based on 'Introductory Guide to Full Licence Requirements' - Version 4 published by the Financial Markets Authority in April 2021 and the standard conditions for full financial advice provider licences. FMA Nov 2020.

Please refer to the information provided and seek advice in relation to meeting the standard conditions specifically for your Financial Advice Provider Licence.

Rules of Use

This Workbook is only for the use of Members of Financial Advice New Zealand Inc (the Association) and may not be distributed, copied, emailed, or transmitted to parties outside the Membership of Financial Advice New Zealand without express and written permission from the Association.

This Workbook may contain proprietary or legally privileged information. No privilege is waived or lost by copying, transmission or distribution.

Disclaimer

Nothing in this Workbook represents the views of the FMA or may be construed as advice from the FMA.

Financial Advice New Zealand has made best efforts to ensure the information is accurate and up to date; however, some information in this workbook is noted as time limited.

The Association neither represents warrants nor guarantees that the information and commentary in this Workbook is free of any error or other defect nor does it accept any liability for any loss, cost or damage resulting from reliance on this Workbook.

Financial Advice NEW ZEALAND

PO Box 5513, Wellington 6140

0800 432 101

info@financialadvice.nz