FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

JULY 2023

Consultation: Proposed standard condition on business continuity and technology systems

About this consultation

This consultation proposes a new business continuity and technology systems standard condition for the following types of market service licences:

- Managers of registered schemes (but not restricted schemes);
- Providers of discretionary investment management services;
- Derivatives issuers; and
- Prescribed intermediary services (peer-to-peer lending providers and crowdfunding service providers).

The view of the Financial Markets Authority – Te Mana Tātai Hokohoko (**FMA**) is that the increasing technological risks facing the financial services sector mean it is necessary to ensure holders of these licence types (referred to as 'relevant licence holders') meet minimum business continuity and technology standards. This proposal continues our roll-out of this standard condition across licence types, to reflect the importance of ensuring licence holders are able to continuously provide their market services. By doing so, consumers and investors will have the security of continuity of the relevant services and associated products they receive from market services licensees.

A similar condition is already in place for providers of a financial advice service, and the same standard condition will apply to financial institutions licensed under the Financial Markets Conduct Act 2013 (**FMC Act**), as amended by the Financial Markets (Conduct of Institutions) Amendment Act 2022 (**CoFI Act**).

We welcome feedback on the proposed standard condition discussed in this paper. Please use the feedback form to provide comments. We are seeking general feedback as well as responses to the specific questions in this paper. Submissions close on 1 September 2023. If you have questions about this consultation, please email questions@fma.govt.nz or call us on 0800 434 566 (+64 3 962 2695).

This consultation is for relevant licence holders and interested parties.	It seeks feedback on a proposed standard condition on business continuity and technology systems for relevant licence holders.

Contents

Background 2

Operational resilience 2

Market service licences 2

Proposed standard condition 3

Rationale 5

New standard condition 5

- Market service licence types 5
- Proposed condition obligations 5

Implementation timeframes 7

Questions 8

Feedback form 9

Background

Operational resilience

In recent years we have been looking more closely at the operational resilience of market service licensees. This has been driven mostly by rapidly developing sophistication of cyber threats and the increasing volume of technology incidents and remediation activity reported to the FMA.

Given the financial services sector typically relies heavily on technology, we have heightened our focus on licensed entities' operational resilience, particularly cyber risks:

- In 2019, we published a thematic review of cyber resilience in FMA-regulated entities, which utilised the US National Institute of Standards and Technology's (NIST) Cybersecurity Framework. For this review, participating entities self-assessed their cyber resilience maturity across five core cyber security functions: Identify, Protect, Detect, Respond, and Recover. We found most participants were aware of the increasing cyber security risk, and assessed themselves as being highly capable of protecting against, and recovering from, such threats. However, participating entities did not rate themselves highly in terms of detecting and responding to cyber threats.
- In July 2022, we released an information sheet to assist market services licensees (excluding benchmark administrators) licensed under Part 6 of the FMC Act to enhance the resilience of their cyber security and operational systems. In July 2021, a cyber resilience information sheet was released to assist financial advice providers (**FAPs**) to develop their cyber resilience.

We recognise that operational resilience is wider than cyber resilience. One of the key steps to reduce the extent and likelihood of disruption to market services is for licensed entities to have and maintain a business continuity plan (**BCP**). There are unique features of cyber-related risks that we consider need additional oversight and earlier notification than other types of operational risks.

Market service licences

The FMA grants a range of market services licences under Part 6 of the FMC Act.

Licence conditions can be imposed by legislation or regulation, or by the FMA. Conditions are obligations that licence holders, and those authorised under a licence, must comply with. Licence conditions can be standard (i.e. apply to all licences) or specific (i.e. apply to an individual licence holder or authorised body).

Licence conditions may impose limits or restrictions on the services that are covered by the licence, or impose conditions in relation to the licensing requirements. Conditions are necessary to ensure licence holders continue to meet those requirements, and to help us effectively monitor the licensed population.

Currently, only some market services licensees are subject to conditions specific to business continuity and technology systems.

Proposed standard condition

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 market service.
>
> If you use any technology systems, which if disrupted would materially affect the continued provision of your market service (or any other market services licensee obligation), you must at all times ensure the operational resilience of those systems – being the preservation of confidentiality, integrity and availability of information and/or technology systems – is maintained.
>
> You must notify us as soon as possible and, in any case, no later than 72 hours, after discovering any event that materially impacts the operational resilience of your critical technology systems, and provide details of the event and impact on your market service and recipients of the service.

Explanatory note: This condition requires you to have suitable arrangements in place to be able to manage disruptions to your business. This is intended to provide recipients of your financial services with the security of continuity of relevant services and associated products they receive from you.

Your *business continuity plan* includes the documented procedures that guide you to respond, recover, resume and restore a predefined level of operation following disruption. This plan should provide for the continuity of your market service generally – not just the recovery of your technology systems. It should also encompass any outsource arrangements.

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 market service, operational arrangements and exposure to disruptive events.

A small market services licensee with simple processes and technology may only need a relatively brief plan covering a more limited range of likely disruptive events. A larger or more complex market services licensee, 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 size or 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 market service or your ability to meet your licensee obligations.

This condition requires that you maintain the operational resilience of your critical technology. This includes:

a) regularly identifying and reviewing your operational risks, including cyber risk and threats; and

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

c) having effective processes that monitor and detect activity that impacts your operational resilience; and

d) setting out in your business continuity plan your predetermined procedures for responding to, and recovering from, events that impact on your operational resilience.

The operational resilience 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 framework for this purpose.

You must have arrangements in place to notify us after discovering any event that materially impacts the operational resilience of your critical technology systems. This includes any technological or cyber security event that materially disrupts or affects the provision of your market service, or has a material adverse impact on recipients of the service. You do not need to notify us of minor events, such as receiving a 'phishing' email that is not successful i.e. has not materially disrupted or affected the provision of your market service, and has not had a material adverse impact on recipients of the service.

You need to provide details of the event including the affected systems, and the impact on your market service and recipients of the service. This should also include projected recovery timelines and remediation activity. If some of the details are not available at the time you discover the event, you will need to provide these details to us as soon as possible. We may also request additional information about the event. We may also specify the format or additional requirements for notifying events to the FMA.

Rationale

New standard condition

Market service licence types

For this consultation, we are proposing to roll out a business continuity and technology systems standard condition to these Part 6 licence types:

- managers of registered schemes (other than a restricted scheme);
- providers of discretionary investment management services;
- derivatives issuers;
- peer-to-peer lending providers; and
- crowdfunding service providers.

To avoid doubt, the proposed condition is not proposed to apply to the following Part 6 licence types:

- Benchmark administrators, which have existing technology-related obligations under the Financial Markets Conduct Regulations 2014.
- Licensed Independent Trustees, who are individuals who form part of the manager of a restricted scheme as an individual trustee or as the director of a corporate trustee.

The roll out has been staged due to the timing of key legislative changes in recent years. In 2020, we consulted on, and imposed, a new standard condition specifically related to business continuity and technology systems on licensed FAPs as part of the change in the financial advice regime under the Financial Services Legislation Amendment Act 2019. The FAP standard condition is similar to the proposed standard condition outlined in this paper, with the main difference being the notification period (see below).

In 2022, we consulted on a similar standard condition for a licence under the CoFI Act regime, which was finalised and will apply to financial institutions.

We recognise that for many market service providers, service delivery involves third parties, e.g. providers of trade execution, portfolio administration, reporting, or custodial services (including supervisors). The proposed condition recognises that it is the licensed market services provider that is ultimately responsible for delivering its market services, and we would expect the licensee to have systems and processes in place to allow it to give effect to the proposed condition.

Proposed condition obligations

Background

The FMA may add to the conditions of a licence at any time after the licence is issued, to impose conditions relating to the requirements referred to in ss 396 or 400 of the FMC Act (for example, to ensure that those

requirements continue to be satisfied and to require verification that those requirements continue to be satisfied).

The types of market service licences to which this consultation is related are subject to a standard condition on compliance, which requires them to have, at all times, adequate and effective systems, policies, processes and controls that are likely to ensure they will meet market services licensee obligations in an effective manner.

Additionally, to be licensed, these entities must meet the minimum standard for operational infrastructure as outlined in the licensing guide for each licence type. This covers having IT systems to deliver the licensed market service that are secure and reliable, and arrangements to ensure the IT systems perform the intended processes efficiently. It also includes ensuring associated risks are managed, as well as having a business continuity plan that provides for the continuity of business operations generally – not just the recovery of IT systems.[1]

With reference to s 403(3)(b) of the FMC Act, we consider that it is necessary and desirable to add to the standard conditions of these licences to ensure licence holders continue to be capable of effectively performing their market service with reference to the specific matters about IT security and business continuity the FMA relied on in deciding to issue the licence.

The purpose of this standard condition is to:

- ensure licence holders maintain business continuity plans; and
- ensure there are appropriate ongoing obligations to maintain the operational resilience of technology systems; and
- require licence holders to notify the FMA about material disruptions to their critical technology systems.

Business continuity plans

The proposed condition requires licence holders to have an appropriate and regularly tested BCP. BCPs enable entities to be prepared to respond to and recover from an event that disrupts their market service.

The condition does not prescribe the scope or details of the BCP. Licence holders must consider their own structures and arrangements, and the disruptive risks that could impact them. Where a licence holder relies on technology systems as a core part of providing its service or to meet its licensee obligations, the condition requires that these critical technology systems must be secure, reliable and addressed as part of business continuity planning.

BCPs are necessarily broader than technology systems. BCPs are already required as part of the licensing process, where they form part of the minimum licensing standard related to IT systems and business continuity.

This standard condition aligns with that minimum standard and ensures that relevant licence holders have, on an ongoing basis, appropriate business continuity and technology systems to remain capable of effectively carrying out their licensed service.

[1] For example see pages 34-35 of Part B3 of the Licensing Application Guide for managed investment scheme managers

Technology systems

We recognise the specific threat that material disruptions to technology systems may pose to licensees delivering market services. The proposed standard condition addresses this in the following ways:

- It places an obligation on licence holders to at all times ensure the operational resilience of technology systems which, if disrupted, would materially affect the continued provision of the licensee's market service (or any other market service licensee obligation). The obligation extends to ensuring the preservation of confidentiality, integrity and availability of information and/or technology systems is maintained.
- It also introduces a new notification obligation, requiring the entity to notify the FMA as soon as possible and, in any case, no later than 72 hours, after discovering any event that materially impacts the operational resilience of the licensee's critical technology systems. This includes an event that materially disrupts or affects the provision of the licensee's market service or has a material adverse impact on recipients of those services (e.g. consumers or investors).

The 72-hour period is shorter than the 10-working-day period notification requirement under the standard condition for FAPs. This reflects the reliance on technology by the relevant licence holders and the likelihood of harm to consumers and investors when disruptions occur. It also reflects the significance of technology in maintaining sound and efficient financial markets.

The 72-hour period is the same as the notification requirement that will apply to financial institution licences.

Disruption to financial services, even for a short period of time, can have a detrimental impact on recipients of the service. Timely reporting of an event of the nature set out in the standard condition will ensure the FMA is kept informed of the event and can respond effectively should the need arise. The 72-hour period aligns with the reporting requirements imposed by other financial regulators, including the proposed mandatory reporting requirements for material cyber incidents by the Reserve Bank of New Zealand.

We also note there is a difference in terminology between the proposed standard condition ("operational resilience") and the standard condition for FAPs ("information security"). We intend the standard conditions to be broadly aligned, as the focus is on entities to manage disruptions to their technology systems and be more than just cyber security related. The aim is for entities to provide for the continuity of their financial services generally – not just the recovery of technology systems.

Implementation timeframes

We are also seeking feedback on whether this proposed standard condition – if we decide to impose it – should come into effect three months after the date that we publish a decision or sooner, e.g. one month after the decision is published.

Most licence holders will already have a BCP and be aware of our expectation that entities should notify the FMA of any technological or cyber security event that materially disrupts or affects the provision of their regulated services,[2] so our preference is for the condition to take effect shortly after a decision is published.

[2] See the FMA's *Cyber Security and Operational Systems Resilience Guidance* (June 2022) at pg 6.

Questions

1. Do you agree or disagree with the proposed standard condition? Please provide your reasons.
2. Do you consider you will need to make material changes to your existing business continuity plan as a result of the proposed condition?
3. Do you rely on critical technology systems to deliver your market service? If not, why do you not consider any of your technology systems to be critical?
4. Do you agree with our intention for the proposed standard condition for current or new licensees to be effective three months after publication of our decision (if we decide to impose a standard condition)? Please provide your reasons.
5. Would the proposed standard condition create any additional compliance costs for your business? If so, please detail those costs.
6. Would the proposed standard condition have any other adverse impacts on your business? If so, please describe what these would be.
7. Does the proposed standard condition create a barrier to enter the market? If so, please explain why this is the case.
8. Do you have any other comments on the proposed standard condition or how it is drafted?

Feedback form

Consultation: Proposed standard condition on business continuity and technology systems

Please submit this feedback form electronically in both PDF and MS Word formats and email it to us at consultation@fma.govt.nz with 'Proposed standard condition on business continuity and technology systems: [your organisation's name]' in the subject line. Thank you. **Submissions close on 1 September 2023**

Date: Number of pages:

Name of submitter:

Company or entity:

Organisation type:

Contact name (if different):

Contact email and phone:

Question number	**Response**

Feedback summary – *if you wish to highlight anything in particular*

Please note: Feedback received is subject to the Official Information Act 1982. We may make submissions available on our website, compile a summary of submissions, or draw attention to individual submissions in internal or external reports. If you want us to withhold any commercially sensitive or proprietary information in your submission, please clearly state this and note the specific section. We will consider your request in line with our obligations under the Official Information Act.

Thank you for your feedback – we appreciate your time and input.