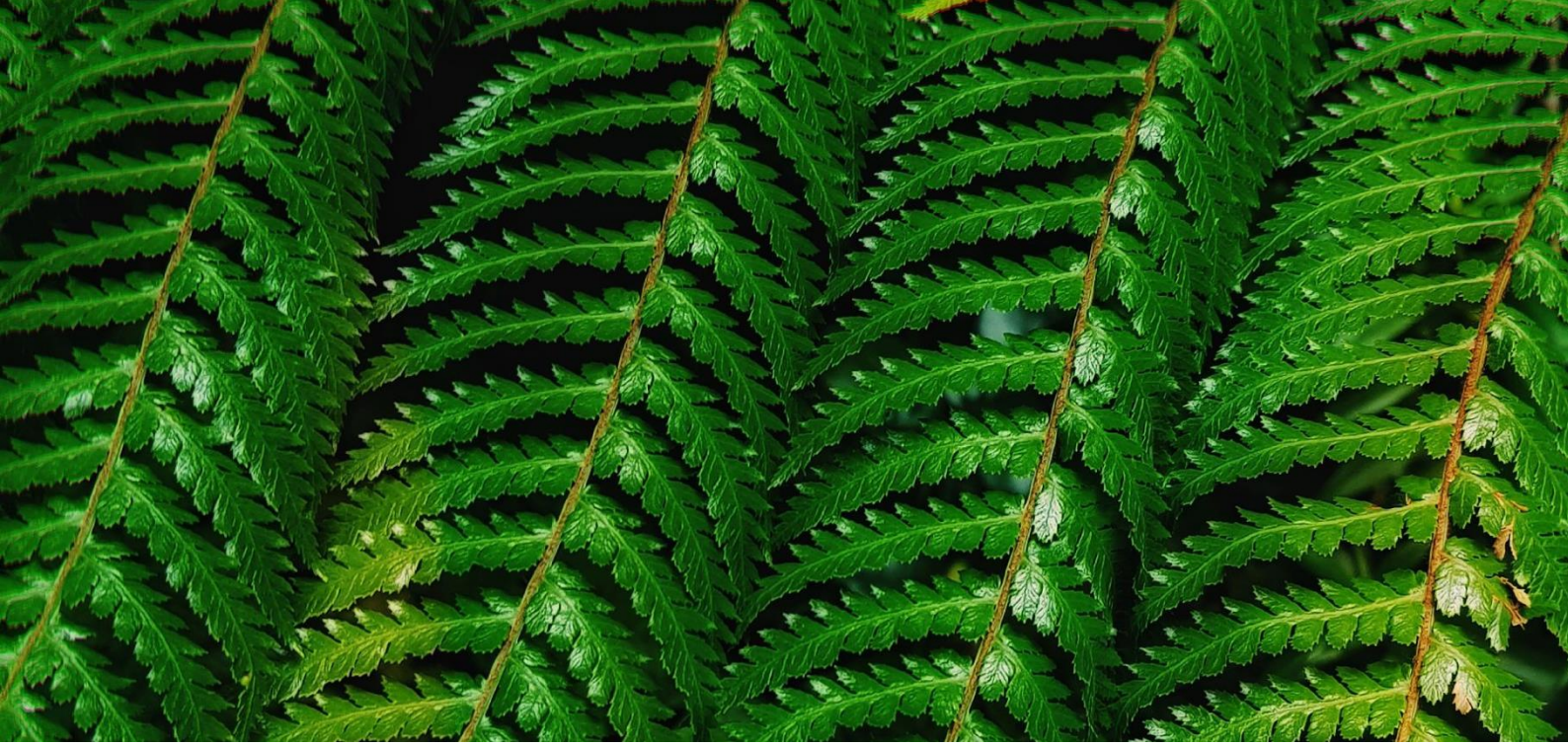

APRIL 2024

Regulatory Impact Statement:

Operational resilience condition for certain market services licence holders under Part 6 of the Financial Markets Conduct Act 2013

This document is for any person that holds one of the following market services licences: manager of a registered scheme, discretionary investment management service, derivatives issuer, peer-to-peer lending and crowdfunding service. It discusses the new standard condition relating to having and maintaining business continuity plans and critical technology systems.

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Contents

Executive summary

Document purpose

This Regulatory Impact Statement (RIS) outlines the decision of the Financial Markets Authority – Te Mana Tātai Hokohoko (FMA) to introduce a new standard condition. The condition relates to business continuity and technology systems, and applies to certain classes of market services licence (under Part 6 of the Financial Markets Conduct Act 2013 (FMC Act)). The condition takes effect on and from **Monday 1 July 2024.**

This RIS summarises the problems we are seeking to address, our objectives, the options and their associated impacts, and the consultation process we undertook before deciding to impose the condition. It also considers whether imposing the condition would be consistent with, and promote, objectives that align with some of the statutory purposes of the FMC Act.

Background

Operational infrastructure and licensing

Managers of registered schemes (other than restricted schemes), discretionary investment management service providers, derivatives issuers (who make regulated offers), peer-to-peer lending providers, and crowdfunding service providers must obtain a licence under Part 6 of the FMC Act to operate.

The FMA's licensing assessment process considers whether the applicant's operational infrastructure meets the licensing application guide's minimum standards for that licence type. Those standards include having documented business continuity plans, and having secure and reliable IT systems to deliver the licensed market service.[1] This is a point-in-time assessment, but licence holders are expected to have and maintain their operational infrastructure at a minimum to the standard presented, and assessed, in the licensing application.

Cyber threats continue to rapidly develop in sophistication and frequency based on increasing reports of technology incidents and remediation activity. Without an express licence condition, the current arrangements are not always suitable to ensure the FMA is informed about unfolding cyber threats. It is not necessarily clear how or when, in the context of that type of event, the mandatory reporting obligation in s 412(2) of the FMC Act would apply.

We consider improved regulatory oversight is needed to help ensure businesses continue to maintain and review their business continuity plans, and have secure and reliable IT systems to deliver their licensed market services.

[1] You can read more under the "Operational Infrastructure" section of the minimum standards in the licensing guide for each of those licence types.

Specific licence condition for business continuity and critical technology systems

Licence conditions are an important and necessary part of maintaining ongoing regulatory standards and helping us to effectively supervise the licensed population. Licence holders (and those authorised under the licence) must comply with them. Conditions are imposed by legislation automatically[2] and by the FMA. The FMA conditions can apply to all licences of a class (referred to as standard conditions) or to an individual entity (referred to as specific conditions).

We have developed a new standard condition that has an express obligation to have and maintain appropriate business continuity plans and critical technology systems. It also requires licence holders to notify the FMA as soon as possible but no later than 72 hours after discovering an event that materially impacts those critical technology systems. To facilitate the notification process, we are currently developing an online notification template. It is intended to allow rapid notification of essential information, followed by updates as information becomes clearer.

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

This new condition and the CoFI condition will have a 72-hour notification period. This is necessarily much shorter than the 10 working days under the FAP condition, to reflect 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.

Consultation process

Between July and September 2023, we consulted on this issue, described in our consultation paper *Consultation: Proposed standard condition on business continuity and technology systems*, seeking feedback on our proposal to impose a standard condition on business continuity and technology systems. In December 2023, we gave written notice under s 405 of the FMC Act to those licence holders affected by this new standard condition. We have set out the key themes from the public consultation process and the written notice in this RIS.

Dual FMA/RBNZ regulated entities

We have worked with the Reserve Bank of New Zealand (RBNZ) in developing the new standard condition, and the reporting thresholds for this standard condition and the RBNZ's cyber resilience condition. We will continue to make refinements and improvements to maximise regulatory efficiency and minimise regulatory burden on licence holders.

[2] The FMC Act and the Financial Markets Conduct Regulations 2014

Objectives and relevant stakeholders

Objectives

We want to ensure that:

- licence holders have and maintain appropriate business continuity plans, and maintain the operational resilience of their critical technology systems
- the FMA is made aware in a timely way of material incidents impacting critical technology amongst market services licensees.

These objectives are consistent with, and promote, some of the purposes of the FMC Act – being to avoid unnecessary compliance costs; promote the confident and informed participation of businesses, investors, and consumers in the financial markets; and promote and facilitate the development of fair, efficient, and transparent financial markets.

We have used these objectives to assess the key options, as set out in this RIS.

Relevant stakeholders

The standard condition will impose new obligations on persons who are, or have been, granted certain market services licences under Part 6 of the FMC Act, being:

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

Problem definition, options, and impact analysis

Problem definition

The FMA generally has limited regulatory oversight of whether, or to what extent, licence holders are maintaining business continuity plans and critical technology systems after a licence is granted. The FMA relies on market surveillance, voluntary reporting, and mandatory s 412 reporting[3] to remain informed about technology risks and cyber incidents affecting aspects of financial services and products offered in New Zealand. It is also difficult for the FMA to take effective regulatory action in response to issues with those plans or systems without an express obligation on the regulated entities to have and to maintain those systems or plans.

Consumers, businesses and investors who use or rely on the market services ultimately carry the risk of loss or harm where business continuity plans are inadequately tested and maintained, or critical technology systems are not resilient. That loss or harm may be permanent or temporary loss of access to, or timely information about, assets or investments, or loss of personal and financial information to unauthorised third parties. Such incidents also reduce confidence in the financial sector.

Options

We considered three options in relation to the new condition:

- Option 1: Status quo (No condition)
- Option 2: Add condition as consulted on (**Preferred option**)
- Option 3: Add condition with extended notification timeframe

[3] Section 412(3) of the FMC Act requires every licensee to report to the FMA if they have contravened, may have contravened, or are likely to have contravened a market services licensee obligation in a material respect, or if a material change of circumstances has occurred, may have occurred or is likely to occur in relation to a licence (amongst other matters).

Option 1: Status quo (No condition)

Description

Option 1 continues the status quo by not imposing a business continuity and technology systems requirement as a licence condition but could involve the FMA providing further guidance about its expectations.

Impact analysis

Overall, this option is more likely to result in poor outcomes for consumers, investors, businesses and markets, and does not very effectively support the purposes of the FMC Act.

Regulatory burden

Applicants for a market services licence must already have suitable business continuity plans and appropriate IT systems before the FMA grants a licence. Licence holders need to maintain these plans and systems to the same or equivalent standard to that presented in their licence application. This is also good business practice.

Protection for consumers, investors, and businesses

Consumers, investors, and businesses using the services of licensed market service providers ultimately carry the risk where the service provider's assets, information, or access to a licensed service may be compromised or lost because of a material disruption to the business or its critical technology systems. Under Option 1, we think there is a higher likelihood that more licensed persons will not maintain business continuity plans or critical technology systems to an appropriate standard. This in turn increases the risk for harm flowing from any failure to deliver licensed market services.

Regulatory oversight

The FMA has market visibility of general threats to business continuity and operational resilience, and cyber risks through proactive and reactive monitoring. Licence holders must also report incidents (e.g. material change of circumstances) to the FMA under s 412 of the FMC Act and may notify us about incidents below that threshold.

Option 1 is likely to mean we do not have up-to-date information to allow effective regulatory oversight. For example, current and emerging high-risk technology threats are borderless and can move rapidly internationally and domestically. At its most serious, consumer and investor assets can be compromised and moved offshore.

The mandatory reporting obligation in s 412(3) of the FMC Act has not been successful for effective reporting of cyber risks. This may be because:

- It can be difficult for a licensee to form a view about when and if a cyber risk, as it is unfolding, meets the relevant thresholds of possibly contravening a market services licensee obligation or there is likely to be a material change of circumstances under s 412(2).
- The timeframe for reporting a matter, assuming it meets s 412(2), is "as soon as practicable after the licensee forms the belief", which is not necessarily suitable for cyber risks (where time is of the essence).

Further, MIS managers report only to MIS supervisors (not the FMA) in certain circumstances.

Overall, regulatory oversight is not likely to be at an appropriate level for sectors where risk to consumers is the highest from a market service outage or system compromise.

Option 2: Add standard condition as consulted on (preferred option)

Description

Option 2 is to impose a standard condition on relevant licence holders that requires them to have and maintain a business continuity plan appropriate for the scale and scope of the licensed service, which includes maintaining the operational resilience of critical technology systems, and a requirement to notify the FMA of events that materially impact the operational resilience of critical technology systems.

Impact analysis

Regulatory burden

To be granted a licence, entities must already have business continuity plans and IT systems with effective safeguards and backups proportionate to the size and complexity of the business, its licensed market services, and its operational risk profile. This part of the condition does not impose a new regulatory burden.

Licence holders will already have processes and procedures in place to fulfil their s 412 obligations. However, there is a one-off impact while licence holders make specific updates to their systems, processes, and policies to meet the requirements of the new standard condition (particularly the time limit). There is a small additional burden to notify the FMA when an event occurs. As discussed below, some submitters said the 72-hour reporting period for these events is too short. The proposed online notification process will aid reporting by including key information that will be requested at the time of reporting and provide instructions on what is expected of licence holders. Early notification is critical because cyber-related risks are often time sensitive.

Protection for consumers, investors, and businesses

Consumers, investors and businesses are likely to be better protected under Option 2. Adding a licence condition signals the importance of operational resilience when providing licensed market services. We think this is more likely to lead to improved and more appropriately prioritised efforts to have and maintain business continuity plans and the resilience of critical technology systems. In turn, this improves the likelihood of the continuity of licensed market services and the protection of consumer and investor assets and information.

Regulatory oversight

Option 2 is likely to significantly improve the scope and timeliness of information disclosure about operational resilience, which will improve our ability to identify and monitor cross-market threats (within these licence classes, and across FAPs and financial institutions under CoFI, which have this condition). This also helps us act on, and exchange, descriptions of emerging threats with domestic and international counterparts, given the borderless and rapid pace of certain types of attack.

Option 2 also makes it clear that the FMA will look more closely at the adequacy of business continuity plans and maintaining critical technology systems.

Option 3: Add standard condition with extended notification timeframe

Description

Option 3 is to impose the standard condition with an obligation to notify the FMA as soon as possible but not later than 5 working days after discovering any event that materially impacts the operational resilience of the licence holder's critical technology systems.

Impact analysis

Regulatory burden

We do not consider there is any material difference between the regulatory burden of Option 2 and Option 3.

Protection for consumers, investors, and businesses

There is an increased risk to consumers, investors and businesses that participate in financial markets in some scenarios, i.e. where issues are not reported to the FMA at the earliest opportunity. This could increase the risk of irreversible harm to market service providers or consumer assets or data, and delay regulator awareness of potentially systemic issues (e.g. when connected to international misconduct).

Regulatory oversight

As above, an extended notification period reduces regulatory oversight. It may compromise our ability to be informed about critical market impacts promptly and the ability of our counterpart agencies to carry out any necessary actions promptly, and ability to check risk trends in the licensed sectors.

Summary of assessment of options against objectives

We have assessed the options against the criteria below.

Key: ✓✓ Meets the policy objectives | ✓ Partially meets the policy objectives | ✗ Does not meet the policy objectives

Criteria	Ensures appropriate operational resilience in the licensed population	Promoting the confident and informed participation of businesses, investors and consumers in the financial markets	Promoting and facilitating the development of fair, efficient, and transparent financial markets	Avoiding unnecessary compliance costs
Option 1: No condition (status quo)	Low to moderate likelihood of some licence holders not adequately maintaining business continuity plans or critical technology systems, and being unable to effectively respond to and recover from an event that disrupts their business. ✗	A serious event undermines confident participation in financial markets for businesses, investors and consumers alike (for example through potential for loss of assets or personal information). This probability is higher where certain licence holders are below the expected standard. ✗	As for the previous column in this option, serious events may result in, for example, the inability for customers to view or trade assets, or to buy or sell instruments to hedge risk, which negatively affects the efficiency of financial markets. This probability is higher under Option 1. ✗	No additional compliance costs for licence holders. ✓✓
Option 2: Imposing condition as consulted on (preferred)	Improved regulatory oversight, and clear requirement is expected to reduce likelihood of non- or poor compliance. Obligation to notify FMA obliges firms to have proper escalation processes, and reporting information helps FMA support operational resilience in the market. ✓✓	Improved compliance reduces frequency and/or impact of disruptive events. Notification allows FMA to monitor and report on aggregate trends and risks, which promotes the confident and informed participation of businesses, investors and consumers in the financial markets. ✓✓	As for previous criteria, fewer or less-impactful disruptive events helps facilitate efficient financial markets. Notifying material incidents to FMA promotes transparency in the financial markets. ✓✓	Minor additional compliance costs relating to having timely notification processes. Licence holders already have business continuity plans and IT systems (considered as part of licensing) and processes for s 412 notifications. ✓✓

Criteria	Ensures appropriate operational resilience in the licensed population	Promoting the confident and informed participation of businesses, investors and consumers in the financial markets	Promoting and facilitating the development of fair, efficient, and transparent financial markets	Avoiding unnecessary compliance costs
Option 3: Imposing condition with modified notification timeframe	As in Option 2 above. ✓✓	As in Option 2 above. A 5-day notification window compromises efficacy of monitoring, oversight and response, as time is of the essence for the most critical threats – particularly where regulatory intervention can minimise harm. ✓	As in Option 2 above. Delayed notification compromises efficacy of monitoring, oversight and response, as time is of the essence for the most critical threats. ✓	As in Option 2 above, minor additional compliance costs. ✓✓

Consultation process and themes

In July 2023, we released a consultation paper *Proposed standard condition for licence holders under Part 6 of the FMC Act*, seeking feedback on our proposal to impose a standard condition on business continuity and technology systems for certain market services licence holders. This condition is set out in Schedule 1.

We received 12 written submissions from a range of stakeholders including industry bodies, licence holders, and a law firm. We carefully considered the feedback, and in December 2023 issued written notice that we may impose the standard condition on relevant licensees under s 405 of the FMC Act. Key themes from the public consultation and additional feedback received in response to the notice are outlined below.

A collation of submissions on the public consultation is available from the consultation web page.

Key themes

All submitters agreed in principle with both the new standard condition on business continuity and technology systems, and the FMA's view that the increasing technological risks facing the financial services sector mean it is necessary to ensure holders of these licence types meet minimum business continuity and technology standards.

Key submissions

Business continuity

No public consultation submitters believed any material changes to their existing plans would be required if the condition were imposed. One requested express confirmation that licence holders retain responsibility for any outsourcing arrangements. One asked for guidance on which frameworks would be recognised for the purpose of the condition.

We have made no changes to the first paragraph of the condition, which relates to business continuity plans. It is an express licence condition that licence holders are responsible for outsourced arrangements. We encourage entities to use an appropriate framework, in line with the scale and scope of their business, to assist with planning, prioritising and managing their operational risk (including cyber risk).

Notification

Almost all public consultation submitters, and a small number of notification respondents, had comments about the 72-hour notification period.

Longer notification period:

- *Some submitters preferred a working day timeframe and noted potential delays gathering third-party information for the notification. Three asked for a longer timeframe. One said the timeframe should*

only be in a best-practice guide. Two said the proposed timeframe should be consistent with the required timeframe (10 working days) for FAPs.

Technology outages and cyber-attacks can cause material disruptions that have a detrimental impact on effective provision of the service. Timely reporting of material incidents ensures we are made aware of issues and can monitor these to ensure disruptions are addressed in a timely manner and that customers are treated fairly in the process. Given these disruptions could arise from cross-border cyber incidents and third-party service provider dependencies, a working-day timeframe is not suitable (and adds complexity where an event occurs on a weekend or public holiday).

We have also considered a longer timeframe (5 working days) for notification as part of our options analysis above, and consider that it is important to remain consistent with international best practice and to ensure a clear timeframe for reporting, for consistency across FMA licensees, particularly where loss of data or assets is a key risk.

Therefore, we consider the 72-hour timeframe (which also features in the CoFI licence standard) is appropriate for these Part 6 licensed market services.

Materiality:

- *Three submitters asked for clarification about when the notification period begins (i.e. it may not be immediately clear whether or not an event has or will have a material impact). Three asked for a definition of "materiality".*

  We do not consider it desirable for the FMA to prescribe this detail in a condition. In terms of timing, licence holders must only report after deciding the event is materially affecting the operational resilience of their critical technology systems.

  In terms of "materiality", every incident is different. Licence holders are best placed to ensure their internal systems and guidelines allow them to decide the significance of an event. This should include factors like the size and structure of the organisation, the nature and magnitude of the event, and the impact on the business and customers. It will not include planned system outages, unless there is an unintended consequence that has a material impact.

  We may clarify our expectations in guidance later.

Secure notification platform or template:

- *Two submitters asked for a secure notification platform or online template.*

  We are currently considering appropriately secure options for reporting tools that can be used by licence holders to notify the FMA.

Detail in notification:

- *Four submitters wanted clarity on the details to be notified to the FMA. Two noted the requirements appeared inconsistent with the standard conditions for financial institutions (under CoFI) and FAPs*

(the latter having 10 working days). One noted, if full details are needed, notification post-resolution would not divert resources from responding to the incident.

The notification template has been developed. It will be intended to allow rapid notification of essential information, followed by updates as information becomes clearer.

Overlap with mandatory s 412(3) reporting:

- *One submitter considered the notification requirement overlaps with s 412(3) and a timeframe is not consistent with this statutory requirement.*

  The notification is targeting a specific type of incident that is critical to the licence holder's ability to carry out its licensed market services.

  We consider there are a range of instances where the s 412(3) reporting duty is insufficient to provide an appropriate level of regulatory oversight. This includes where there is a materially impactful event, and the licence holder decides that no breach of licensed market service obligations is likely to occur or there is no material change of circumstances.

  In addition, MIS managers provide s 412(3) reports to the MIS supervisor, not to the FMA, in certain circumstances, and we consider that it is important for the FMA to be notified of this type of material impact directly given the potential systemic implications and need for streamlined reporting.

Critical technology

All public consultation submitters that provide licensed market services confirmed that they rely on critical technology to deliver those services. Two submitters on the notification were concerned the standard of "ensuring … operational resilience" in the second paragraph of the proposed condition implied an absolute requirement for fail-safe systems.

We consider the condition and guidance text explains that ensuring operational resilience relates to the ongoing process of identifying, detecting, mitigating, responding to and recovering from risks. We have made no changes to the second paragraph of the condition, which relates to critical technology systems.

Implementation period

We consulted on a 3-month period, from when the FMA made and communicated a decision, for the proposed condition to come into effect. This was because relevant licence holders are expected to already comply with the core obligations. Some submitters noted that further time may be needed to make any process and system changes. As a result, in the notice of intention (issued in December 2023), we proposed an implementation date of 1 July 2024.

Conclusion and reasons

We consider that imposing a condition (Option 2) will best achieve the stated objectives. It will ensure that licence holders have and maintain business continuity plans and the operational resilience of their critical technology systems, and support the FMA to more effectively provide regulatory oversight without imposing unnecessary compliance costs.

Continuing the status quo (Option 1) would be unlikely to achieve the stated objectives and has a higher likelihood that parts of the licensed market services sector are under-prepared for business continuity and cyber risks.

Option 2 ensures a focus on business continuity and operational resilience by requiring licensed market service providers to notify the FMA within a suitable period about material incidents affecting critical technology systems. This obligation is important to ensure we are made aware promptly of incidents affecting licensed market services, which can be time-critical given the nature of serious events. We will provide a secure online portal for notifications. The form is intended to be light-touch and, for RBNZ regulated entities, compatible with the cyber incident notification process.

We consider this additional regulatory burden is outweighed by the benefits of the information and oversight the notifications will provide the FMA about the performance of licence holder obligations and the improved ability to monitor market-wide threat trends and respond where appropriate.

We do not consider that an extended notification timeframe (Option 3) is the most suitable option. In the minority of incidents that have potential for system-wide impact, time is critical.

Overall, Option 2 will help to improve the operational resilience of relevant licence holders. It will also help the FMA to be better positioned to monitor and identify threats to licence holders' ability to provide their market services, identify emerging systemic risks, and take any necessary compliance or regulatory action.

Schedule 1

Standard condition for business continuity and technology systems

Standard Condition: *(This standard condition will be effective from 1 July 2024)*

You must have and maintain a business continuity plan that is appropriate for the scale and scope of your licensed 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 licensed 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 licensed market service 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 licensed 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:

- regularly identifying and reviewing your operational risks, including cyber risk and threats; and
- implementing measures that maintain the level of operational resilience necessary for your risk profile; and
- having effective processes that monitor and detect activity that impacts your operational resilience; and
- 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.

AUCKLAND – Level 5, Ernst & Young Building | 2 Takutai Square, Britomart | PO Box 106 672 | Auckland 1143
WELLINGTON – Level 2 | 1 Grey Street | PO Box 1179 | Wellington 6140

fma.govt.nz