FMI STANDARD 17C: CYBER RESILIENCE

17C

Reserve Bank of New Zealand
Te Pūtea Matua

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Ref #20368281 v1.0

DOCUMENT VERSION HISTORY

1 March 2024	First issue date

INTRODUCTION

Application

i. This standard applies to every operator of a designated FMI that was specified in its designation notice under section 29(2)(f) of the Financial Market Infrastructures Act 2021 (the **Act**) as falling within one or more of the following classes of designated FMIs:

(a) a pure payment system; or

(b) a central securities depository; or

(c) a securities settlement system; or

(d) a central counterparty.

Legal powers

ii. Under section 8 of the Act the regulator is defined as the RBNZ and the FMA acting jointly (or the RBNZ acting on its own in relation to pure payment systems).

iii. Section 12 of the Act provides the regulator's functions. These include regulating designated FMIs, dealing with designated systemically important FMIs that are distressed, and other functions under the Act.

iv. Subject to certain statutory prerequisites, section 31 of the Act empowers the regulator to make standards for designated FMIs.

v. Section 34 sets out the matters that standards may deal with or otherwise relate to. Section 34(1)(e)(vii) provides that a standard may deal with, or otherwise relate to, the management by operators of cybersecurity risk.

Interpretation

vi. Words and phrases used in this standard have the same meaning as in the Act.

vii. **Applicable auditing and assurance standards** has the same meaning as in section 5(1) of the Financial Reporting Act 2013.

viii. **Cyber** means relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

ix. **Cyber event** means any observable occurrence in an information system. Cyber events sometimes provide an indication that a cyber incident is occurring.

x. **Cyber incident** means a cyber event that:

(a) jeopardises the cybersecurity of an information system or the information the system processes, stores, or transmits; or

(b) violates the security policies, security procedures, or acceptable use

policies, whether resulting from malicious activity or not.

xi. **Cyber resilience** means the ability of an entity to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents.

xii. **Cyber resilience framework** means the policies, procedures, and internal systems an entity has established to identify, protect, detect, respond to, and recover from the plausible sources of cyber risks it faces.

xiii. **Cyber resilience strategy** means an entity's high-level principles and medium-term plans to achieve its objective of managing cyber risk.

xiv. **Cyber risk** means the combination of the probability of cyber incidents occurring and their impact.

xv. **Cyber risk appetite** means the level of tolerance that an entity has for cyber risk. It includes how much cyber risk an entity is willing to tolerate, and how much an entity is willing to invest or spend to manage the risk.

xvi. **Cyber risk tolerance** means the level of cyber risk an entity is willing to assume.

xvii. **Internal systems** means mechanisms within an FMI or operator to implement policies, procedures, or controls.

xviii. **Qualified auditor** means any of the following:

(a) a licensed auditor as defined in section 6(1) of the Auditor Regulation Act 2011; or

(b) a registered audit firm as defined in section 6(1) of the Auditor Regulation Act 2011; or

(c) the Auditor-General as defined in section 4 of the Public Audit Act 2001.

Commencement

xix. This standard comes into force on 1 March 2024.

REQUIREMENTS

1) An operator must ensure that the FMI maintains cyber resilience in a manner that is commensurate with the FMI's exposure to cyber risk, and enables the FMI to remain sound and efficient.

Cyber resilience strategy and framework

2) Further to the requirements in clause (1), an operator must ensure that the FMI has a cyber resilience strategy and cyber resilience framework that is comprehensive, adequate, and credible. The operator must ensure that the cyber resilience strategy and cyber resilience framework:

    a) are based on internationally and nationally recognised frameworks and guidelines; and

    b) align with the FMI's business objectives, stakeholder requirements, corporate strategy, risk management framework, and other related strategies and frameworks; and

    c) are commensurate with the FMI's cyber risk tolerance, cyber risk appetite, and the operational reliability objectives required under *Standard 17: 'Operational risk'*; and

    d) identify and assess the cyber risk associated with the use of third-party service providers, and outline how this risk will be managed, including through compliance with the requirements in *Standard 17B: 'Critical service providers'*; and

    e) set out how information on cyber incidents and threats will be securely shared with relevant external stakeholders, including the regulator and participants; and

    f) provide for cyber resilience training to staff members (the content of which will depend on the nature of the role) during the entire employment lifecycle; and

    g) are reviewed annually, and updated when required, to ensure that any changes in the cyber risk environment are adequately managed.

Governance of cyber risk management

3) Further to the requirements in clause (1) an operator must ensure that its board of directors is ultimately responsible for the cyber resilience of the FMI. An operator must take reasonable steps to ensure that its board of directors understands the cyber risk environment that the FMI operates in, including ensuring that its board of directors:

    a) appoints a senior manager with the appropriate skills, knowledge, and experience to be accountable for the FMI's cyber resilience strategy and cyber resilience framework; and

    b) ensures that senior management updates the board of directors on any significant changes to the FMI's vulnerabilities or the wider cyber risk environment; and

    c) reviews and approves the FMI's cyber resilience strategy and cyber resilience framework and monitors the implementation of such strategy and framework, including any policies, procedures, and internal systems that support this implementation; and

d) takes responsibility for determining the FMI's cyber risk tolerance and cyber risk appetite.

Review of compliance with the cyber resilience strategy and framework

4) An operator must ensure that the cyber resilience strategy and the cyber resilience framework, and the subsequent compliance with them, are assessed by way of an external assurance engagement by a qualified auditor in accordance with applicable auditing and assurance standards:

    a) at least every two years; and

    b) subject to clause (6), whenever a cyber incident occurs that materially impacts, or could materially impact, the FMI's continuing operations,

5) An operator must provide any report from an external assurance engagement to the regulator at the regulator's request.

6) Clause 4(b) does not apply if, in the opinion of the operator, it is not reasonably practicable to seek an external assessment following a cyber incident that materially impacts, or could materially impact, the FMI's continuing operations.

7) If clause (6) applies, the operator must provide reasons for its opinion to the regulator as soon as possible following the cyber incident.

(See Guidance for Standard 17C: 'Cyber resilience', in Guidance for the FMI Standards for more detail).