Reserve Bank of New Zealand
Te Pūtea Matua

DRAFT FOR CONSULTATION

This RBNZ draft is subject to further changes, including –

- peer review:
- proof reading:
- editorial, minor, and other relevant changes.

This legislation is administered by the Reserve Bank of New Zealand. For more information please see:

Website: https://www.rbnz.govt.nz

Contact phone: 04 472 2029

Contact address: 2 The Terrace, Wellington 6140

Deposit Takers (Operational Resilience) Standard 2027

This standard is made under section 72 of the Deposit Takers Act 2023 by the Reserve Bank of New Zealand after—

(a) complying with section 75(1) of that Act; and

(b) being satisfied of the matters set out in section 72(1) of that Act; and

(c) the board of the Reserve Bank of New Zealand having regard to the matter set out in section 49(1) of the Reserve Bank of New Zealand Act 2021.

Contents

Schedule
Information related to material service providers

Standard

1 Title

This is the Deposit Takers (Operational Resilience) Standard 2027.

2 Commencement

This standard comes into force on 1 December 2028.

Part 1
General provisions

3 Objectives

In line with section 3 of the Act, the objectives of this standard are—

(a) to promote sound, effective, and efficient operational risk practices in the deposit-taking sector to enhance the operational resilience of each deposit taker through the establishment and maintenance of operational risk management frameworks and processes:

(b) to ensure that deposit takers have processes and controls in place to manage operational risks arising from, or in relation to, their—

(i) information and communication technology systems; and

(ii) arrangements with material service providers for critical operations; and

(iii) business continuity planning for critical operations:

(c) to mitigate the impact of operational risks that disrupt deposit takers' critical operations and so ensure business continuity.

4 Interpretation

In this standard, unless the context otherwise requires,—

Act means the Deposit Takers Act 2023

board,—

in relation to a deposit taker incorporated in New Zealand, means a board of directors (or other persons or body exercising powers of management, however described):

(a) in relation to an overseas licensed deposit taker, means the chief executive officer in New Zealand

business continuity plan means a plan of a deposit taker for the continuity of the critical operations of its business that meets the requirements of Part 6

critical operation has the meaning set out in clause 10

ICT system means an organised combination of information and communication technology and related processes together with data that support the delivery of a critical operation, whether the process is digital, manual, or a hybrid process

ICT systems incident management framework has the meaning set out in clause 19(3)

information and communication technology or **ICT** means the technologies for the capture, storage, retrieval, processing, display, representation, organisation, management, security, transfer, and interchange of data and information, including the underlying physical and logical design of individual hardware and software components, and operating environments

material ICT systems incident has the meaning set out in clause 21(1)

material service provider has the meaning set out in clause 22(a)

material service provider arrangement or **MSP arrangement** has the meaning set out in clause 22(b)

operational disruption event means an event or incident that disrupts a deposit taker's critical operations beyond pre-defined tolerance levels

operational risk has the meaning set out in clause 9(1)

risk appetite statement means the statement made by a deposit taker under clause 13 of the Deposit Takers (Risk Management) Standard 2027

security, for the operation of a deposit taker's ICT systems, means the result of protective measures that enable a deposit taker to perform its functions despite risks posed by threats to its use of ICT systems

third party means a person that is not the deposit taker

tolerance level has the meaning set out in clause 11.

5 Application

(1) Parts 2 to 7 apply to—

(a) a deposit taker incorporated in New Zealand:

(b) an overseas licensed deposit taker in relation to its New Zealand business.

(2) Despite subclause (1), for a group 3 deposit taker and an overseas licensed deposit taker, the requirements of the following clauses apply on a diminished basis as indicated in those clauses:

(a) clause 14(1)(c) (in relation to operational risk profiles):

(b) clause 20(2) (in relation to information security control assurance processes):

(c) clause 28(2)(d) and (f) (in relation to business continuity plans):

(d) clause 29(2) (in relation to testing programmes).

6 Approaches to applying and interpreting standard

In meeting a requirement of this standard, a deposit taker must—

(a) determine the steps it takes to meet the requirement in a way that a reasonable person would regard as—

(i) adequate for the requirement; and

(ii) commensurate with the size and nature of the deposit taker's business:

(b) take a comprehensive perspective of risk across all material risk types, whether whole-of-enterprise or group-wide, as applicable.

7 Group requirements

(1) This clause applies—

(a) when a deposit taker incorporated in New Zealand has 1 or more subsidiaries:

(b) to the deposit taker in relation to the group of entities that consists of the deposit taker and its subsidiaries, whether affected by an inclusion or exclusion under subclause (3) or otherwise.

(2) The deposit taker must apply the requirements of this standard on a group-wide basis in cases in which a material operational risk could arise for the group from the business activities or functions of a subsidiary, *see* clause 35.

(3) A condition of a deposit taker's licence may specify a particular entity or class of entities that the deposit taker must include or exclude if the Bank is satisfied that the inclusion or exclusion is necessary or desirable—

(a) to promote the safety and soundness of the deposit taker; or

(b) to avoid or mitigate the adverse effects of the following:

(i) risks to the stability of the financial system:

(ii) risks from the financial system that may damage the broader economy.

8 Reviews and testing programmes

(1) When a deposit taker undertakes a regular review of information, conducts regular testing of processes, or meets any other requirement of this standard on a regular basis, the deposit taker must—

(a) document the results of the review or testing; and

(b) identify and address any weaknesses in the deposit taker's operations in a timely manner.

(2) In relation to a review or testing that is based on an operational risk to which the deposit taker is exposed, the deposit taker may—

(a) unless otherwise expressly stated, choose the optimal frequency or timeline for the review or testing:

(b) conduct the review or testing at a level that reflects the materiality of the risk under consideration.

Part 2
Operational risk and critical operations

9 Meaning of, and requirements for managing, operational risk

(1) For the purposes of this standard, **operational risk**—

(a) means the risk of loss resulting from—

(i) inadequate or failed internal processes, resources, and systems; or

(ii) an external event; and

(b) includes legal risk; and

(c) excludes strategic risk and reputational risk.

(2) This standard sets out the requirements that a deposit taker must meet to manage operational risk and provides, in particular, the requirements for managing the following types of operational risk:

(a) information and communications technology systems (*see* clauses 18 to 21):

(b) MSP arrangements for critical operations (*see* clauses 22 to 26):

(c) business continuity planning for critical operations (*see* clauses 27 to 32).

10 Meaning and identification of critical operations

(1) A deposit taker must—

(a) identify the operations that are critical to its business; and

(b) document those operations.

(2) In this standard, **critical operation** means an operation of the deposit taker or its service provider that, if disrupted beyond tolerance levels, would have a material adverse impact on—

(a) the continued operations of the deposit taker:

(b) the interests of depositors or other customers of the deposit taker:

(c) the role of the deposit taker in the financial system.

(3) The deposit taker must define the following processes as critical operations, if it undertakes them:

(a) the payment of monetary claims:

(b) the acceptance of deposits and ongoing administration of deposits:

(c) custodial services:

(d) settlements:

(e) clearing.

(4) For the avoidance of doubt, the list of processes set out in subclause (3) is a non-exhaustive list of the processes that are critical operations.

11 Tolerance levels for critical operations

(1) For each of its critical operations, a deposit taker must set a tolerance level that establishes the limit within which the deposit taker can accept an operational disruption.

(2) The deposit taker's tolerance level for a critical operation must—

(a) be consistent with the deposit taker's risk appetite statement; and

(b) establish—

(i) the maximum period for which the deposit taker can tolerate a disruption to its operations; or

(ii) the maximum data loss that the deposit taker can accept because of a disruption to its operations; or

(iii) the minimum service levels the deposit taker can maintain while operating under alternative arrangements during a disruption to its operations.

(3) The deposit taker must monitor its compliance with the requirements relating to tolerance levels and report to its board a failure to meet tolerance levels together with a remediation plan.

12 Register of critical operations and material service providers

(1) A deposit taker must establish and maintain a register of—

(a) its critical operations and their associated tolerance levels; and

(b) its material service providers.

(2) The deposit taker must provide the register to the Bank—

(a) when it enters into a new arrangement with a material service provider; or

(b) on request by the Bank.

(3) In compiling the register, the deposit taker must—

(a) use the template provided by the Bank that is available on the Internet site maintained by the Bank:

(b) in relation to material service providers, include in the register the information listed in the schedule.

(4) The deposit taker must—

(a) review and update the register at least once in a 12-month period; and

(b) enter the details of any new material service provider arrangement in the register; and

(c) document any material changes to existing arrangements.

Part 3

Operational risk management frameworks

13 Operational risk management frameworks

(1) To ensure a clear understanding of the operational risks it faces, a deposit taker must establish and maintain an operational risk management framework.

(2) A deposit taker's operational risk management framework is the totality of the deposit taker's systems, structures, policies, processes, and people that enable it to identify, measure, evaluate, report on, control, and mitigate operational risks to its business on a timely basis.

(3) For the purposes of establishing and maintaining its operational risk management framework, the board and senior management of the deposit taker must have the skills, experience, and knowledge to—

(a) enable a sound understanding of the current and emerging operational risks to the deposit taker's ICT systems; and

(b) ensure that the deposit taker can effectively manage those risks.

(4) The deposit taker must ensure that its operational risk management framework is consistent with the requirements of the Deposit Takers (Risk Management) Standard 2027.

14 Operational risk profile

(1) For its operational risk management framework, a deposit taker must establish and maintain an assessment of its operational risk profile that—

(a) is consistent with, and proportionate to, the deposit taker's risk appetite statement; and

(b) sets out the methods for establishing and maintaining its systems, including—

(i) the maintenance of appropriate information systems to monitor operational risk; and

(ii) the compilation and analysis of operational risk data; and

(iii) the identification and documentation of the processes and resources needed to deliver critical operations; and

(c) includes an assessment of the impact of its business and strategic decisions on its operational resilience.

(2) The requirement in subclause (1)(c) does not apply to—

(a) a group 3 deposit taker, as defined in clause 4 of the Deposit Taker (Risk Management) Standard 2027:

(b) an overseas licensed deposit taker.

15 Operational risk practices and internal controls

(1) To manage its operational resilience, a deposit taker must—

(a) consider all operational risks to its business operations, however they may arise:

(b) have processes and controls in place to manage the operational risks.

(2) For the purposes of subclause (1)(b), the deposit taker must design and maintain internal operational risk controls that—

(a) are consistent with, and proportionate to, the deposit taker's risk appetite statement; and

(b) comply with the deposit taker's obligations under the Deposit Takers (Risk Management) Standard 2027.

16 Material operational risk incidents

(1) This clause applies when—

(a) a deposit taker becomes aware of an operational risk incident; and

(b) the deposit taker determines that the incident is likely to have a material adverse impact on—

(i) its financial position; or

(ii) its ability to maintain its critical operations.

(2) A deposit taker must notify the Bank of an operational risk incident as soon as practicable and, in any case, no later than 72 hours after the deposit taker has become aware of it.

(3) For the purposes of subclause (2), the deposit taker must provide any relevant information that it has at the time the incident occurs and, while the situation continues, provide the Bank with updated information on the status of the resolution.

17 Reviews of operational risk management processes, systems, and controls

(1) A deposit taker must regularly monitor, review, and test the effectiveness of its internal operational risk controls.

(2) The results of the review must be provided to the deposit taker's senior management and the issues identified during testing must be addressed in a timely way.

(3) A deposit taker's operational risk management processes and systems must be subject to regular risk-based reviews to ensure they remain fit for purpose.

(4) The reviews referred to in subclause (3) must be conducted by a suitably qualified person with sufficient operational independence.

Part 4

Management of ICT systems risks

18 Managing information and communication technology risks

(1) A deposit taker must establish and maintain processes, controls, and tolerance levels that are appropriate for its operational risk profile to—

(a) support the security of its ICT systems; and

(b) monitor the performance of those systems.

(2) For the purposes of subsection (1), a deposit taker must—

(a) identify and classify the elements of its ICT systems based on criticality:

(b) establish processes and security controls to prevent detect, monitor, respond to, and recover from incidents affecting its ICT systems:

(c) set tolerance levels for its ICT systems that are consistent with—

(i) its operational risk profile under clause 14; and

(ii) its tolerance levels for critical operations under clause 11.

19 ICT systems policy

(1) A deposit taker must have an ICT systems policy to maintain the security of its ICT systems and protect its critical operations.

(2) The ICT systems policy must—

(a) be consistent with the deposit taker's operational risk profile; and

(b) ensure that the deposit taker's ICT systems are capable of adequately responding on a continuing basis to system failures and threats; and

(c) provide for an ICT systems incident management framework and escalation process.

(3) **ICT systems incident management framework** means the arrangements and processes that a deposit taker has in place for responding to an ICT systems incident.

20 Assurance and information-sharing processes

(1) A deposit taker must establish and maintain—

(a) information security controls to ensure that access to information is restricted to authorised persons and assurance processes to ensure that information security controls and information-sharing processes are effective:

(b) information-sharing processes, guided by information security controls, to ensure that information and the method of transmission are shared only after authorised approval.

(2) The assurance processes must—

(a) be adequate to confirm that the controls are effectively responding to evolving threats and vulnerabilities, whether internal or external:

(b) extend to ICT systems provided or maintained by another person:

(c) enable information exchanges for ICT risks with an appropriate external party, such as a regulator or cybersecurity agency:

(d) be cross-referenced to the deposit taker's ICT systems incident management framework for coordination purposes.

(3) The information-sharing processes must clearly define—

(a) the types of information that can be shared; and

(b) the circumstances in which sharing is permitted; and

(c) the appropriate information transmission mechanisms; and

(d) the approvals necessary before information may be shared; and

(e) the methods by which records of information shared and approvals granted will be maintained.

(4) Subclause (2) does not apply to a group 3 deposit taker or an overseas licensed deposit taker.

21 Material ICT systems incidents and control weaknesses

(1) A **material ICT systems incident** is an ICT systems incident that has a material adverse impact or has the potential to have a material adverse impact on the deposit taker or the interests of depositors or other customers, whether financially or otherwise.

(2) A deposit taker must notify the Bank of a material ICT systems incident as soon as practicable and, in any case, no later than 72 hours after it becomes aware of the incident.

(3) When notifying the Bank under subclause (2), the deposit taker must include the following information:

(a) the date on and time at which the incident began or was discovered:

(b) an assessment of the severity of the incident:

(c) the nature and impact of the incident, including any impact on customers, the deposit taker's financial position, and regulatory compliance:

(d) whether a viable solution has been identified.

(4) A deposit taker must also notify the Bank of a material ICT systems control weakness no later than 10 business days after it becomes aware of the weakness.

(5) For the purposes of subclause (4), a material control weakness is a vulnerability in the deposit taker's internal controls that—

(a) is unlikely to be remediated in a timely manner; and

(b) could lead to a material ICT systems incident.

Part 5
Management of risks related to material service providers

22 Meaning of material service provider and MSP arrangement

In this standard, in relation to a deposit taker,—

(a) **material service provider** means a third party that provides a critical operation to the deposit taker:

(b) **material service provider arrangement**, or **MSP arrangement**, means a contractual arrangement between a material service provider and the deposit taker for the provision of critical operations to the deposit taker on a regular or continuing basis.

23 Scope of, and requirements for, MSP arrangements

(1) A deposit taker must ensure that the critical operations undertaken by a material service provider meet the tolerance levels set by the deposit taker for those critical operations.

(2) Before entering into an MSP arrangement, the deposit taker must conduct an adequate inquiry into the ability of the material service provider to meet the requirements of the deposit taker.

(3) For each arrangement, the deposit taker must—

(a) document and monitor the terms of the arrangement, including regularly assessing—

(i) the continuing ability of the material service provider to provide the service to the deposit taker; and

(ii) the business continuity planning capability of the material service provider to ensure that it is appropriate and adequate for the continuation of the arrangement; and

(iii) the risk related to the deposit taker's reliance on the material service provider; and

(b) ensure that the business continuity plan of the deposit taker applies in relation to the material service provider and can be executed if required; and

(c) review any proposal that involves an arrangement for another person to deliver a critical operation to the deposit taker; and

(d) be ready to conduct an orderly exit from the arrangement.

24 Policy for material service provider management

(1) A deposit taker must—

(a) establish a documented policy for the management of its material service providers; and

(b) update the policy on a regular basis.

(2) The policy must document the deposit taker's approaches to—

(a) identifying, managing, and mitigating the operational risks associated with material service providers:

(b) managing its MSP arrangements, including its processes relating to—

(i) the arrangements that it has with material service providers, and how the arrangements are entered into and end:

(ii) how the practices of particular material service providers are monitored:

(iii) how the operational risks associated with particular material service providers are managed:

(c) setting out processes to ensure that the critical operations provided meet the tolerance levels established by the deposit taker:

(d) managing the operational risks associated with a material service provider when the service provider arranges for another person to deliver a critical operation to the deposit taker:

(e) determining the responsibilities of the person who is accountable for managing the deposit taker's MSP arrangements.

25 ICT risks relating to use of material service providers

In relation to the ICT risks posed by a deposit taker's use of material service providers and the range of information that the deposit taker collects and protects, the deposit taker must—

(a) identify and document the information and data collected, stored, or accessed by material service providers of ICT-related critical operations; and

(b) include an assessment of the risks relating to data storage, processing, and transmission, and how the risk identified is to be managed.

26 Reporting requirements

(1) A deposit taker must notify the Bank as soon as practicable of—

(a) the existence of an arrangement with a material service provider; and

(b) any material changes to an existing MSP arrangement; and

(c) the frequency of reports that the board receives under subclause (3).

(2) The reporting requirement in subclause (1)(a) may be made by way of the register established and maintained under clause 12.

(3) The board of the deposit taker, or a designated board committee, as applicable, must be notified about how the MSP arrangements comply with the deposit taker's material service provider management policy under clause 24.

Part 6
Business continuity planning

27 Business continuity plans

(1) A deposit taker must have a business continuity plan for its critical operations in order to—

(a) maintain those operations through defined tolerance levels if an operational disruption event occurs; and

(b) mitigate the impact of the disruption on its business operations.

(2) The business continuity plan must be—

(a) documented and regularly reviewed; and

(b) tested on a regular basis.

(3) A deposit taker must maintain the capabilities required to execute its business continuity plan, including but not limited to access to people, resources, and technology.

28 Contents of business continuity plans

(1) A business continuity plan must set out how a deposit taker is to identify, manage, and respond to an operational disruption event.

(2) The plan must include—

(a) the register established and maintained under clause 12:

(b) a set of documented processes and procedures for determining—

(i) how to identify an operational disruption event:

(ii) what steps are required to activate the plan:

(iii) what arrangements are required to direct the people, technology, or financial resources that are needed to ensure the plan can be activated:

(c) a statement of the actions that the deposit taker must take—

(i) in an operational disruption event to enable it to maintain its critical operations within its tolerance levels; and

(ii) after an operational disruption event to continue its critical operations:

(d) an assessment of the execution risks, required resources, and preparatory measures that the deposit taker needs to support the effective implementation of actions set out in the plan:

(e) for MSP arrangements, a contingency plan to ensure that the deposit taker remains resilient through an operational disruption event:

(f) the documentation of a communications strategy to support the execution of the plan.

(3) The requirements in subclause (2)(d) and (f) do not apply to a group 3 deposit taker or an overseas licensed deposit taker.

29 Regular testing programme

(1) A deposit taker must have a regular programme for testing its business continuity plan that—

(a) covers every critical operation listed in the register; and

(b) focuses on the material risks facing the deposit taker; and

(c) tests the effectiveness of the plan in a range of severe but plausible scenarios.

(2) The deposit taker must conduct a test of its business continuity plan at least once in a 12-month period.

(3) Despite subclause (2), testing of a business continuity plan by a group 3 deposit taker or an overseas licensed deposit taker must be undertaken at least once in a 24-month period.

30 Reviews of business continuity plans

(1) A deposit taker must review its business continuity plan on a regular basis and must update it to reflect any changes in—

(a) its legal or organisational structure:

(b) its business functions or business lines:

(c) its operational risk profile.

(2) The board must be notified of the results of the review on completion. If a review results in material changes, both the board and the Bank must be notified.

31 Assurances relating to business continuity plans

The board must be provided, on a regular basis, with an assurance that the deposit taker's business continuity plan for critical operations—

(a) sets out a credible plan or way in which the deposit taker is to maintain its critical operations within the defined tolerance levels; and

(b) has been adequately tested.

32 Activation of business continuity plans

(1) If a deposit taker activates its business continuity plan for critical operations, it must notify the Bank as soon as practicable and, in any case, no later than 72 hours after activation.

(2) When notifying the Bank, the deposit taker must include the following information:

(a) the nature of the disruption; and

(b) a description of the critical operations affected by the disruption; and

(c) the actions being taken by the deposit taker; and

(d) the likely impact on its business operations; and

(e) the time frame within which it is expected that normal operations will resume.

Part 7
Governance responsibilities

33 Responsibilities of board

(1) It is the responsibility of the board to—

(a) approve the following for the deposit taker:

(i) the tolerance levels for its critical operations (*see* clause 11):

(ii) the operational risk management framework (*see* clause 13):

(iii) the operational risk profile (*see* clause 14):

(iv) the tolerance levels for its ICT systems (*see* clause 18):

(v) the ICT systems policy (*see* clause 19):

(vi) the management policy for its material service providers (*see* clause 24)

(vii) the business continuity plans for critical operations (*see* clause 27):

(b) oversee the deposit taker's processes to implement its operational risk profile, its ICT systems policy, and its management policy for its material service providers.

(2) The board must be notified of the following:

(a) the deposit taker's arrangements with material service providers; and

(b) the deposit taker's business continuity plan for critical operations and any testing of the plan.

34 Responsibilities of senior management

It is the responsibility of senior management to manage the operation of its operational risk management framework, including—

(a) monitoring and managing all operational risks to the deposit taker in a way that is consistent with the policies and processes approved by the board; and

(b) developing the policies and processes in the organisation for approval by the board as described in clause 33.

35 Group governance requirements

(1) This clause applies—

(a) when a deposit taker incorporated in New Zealand has 1 or more subsidiaries:

(b) to the deposit taker in relation to the group of entities that consists of the deposit taker and its subsidiaries, whether affected by an inclusion or exclusion under clause 7(3) or otherwise.

(2) The deposit taker must—

(a) maintain an appropriate operational risk management framework for the group of entities with the aim of mitigating material operational risks, including those relating to ICT systems and material service providers:

(b) ensure that the entities in the group—

(i) have adequate business continuity plans for critical operations that are consistent with group-approved tolerance levels; and

(ii) are able to execute the business continuity plans when required:

(c) notify the Bank as soon as practicable, and in any case, no later than 72 hours after becoming aware of an operational risk incident that is likely—

(i) to have a material financial impact on an entity in the group; or

(ii) to affect the ability of entities in the group to maintain critical operations.

cl 12

Schedule
Information related to material service providers

1 Information

The information that a deposit taker must include in the register for its material service providers under clause 12 is the following:

(a) the legal name, business number, physical address, and address for service, of the material service provider that is providing the critical operations:

(b) the name and contact details of the individual who is accountable for the material service provider:

(c) the location of data related to the deposit taker's critical operations, and an overview of the service, functions, and critical operations covered by the arrangement and the tolerance levels for those critical operations:

(d) the expiry date, and any renewal date, of the material service provider arrangement:

(e) an indication of the materiality of and the deposit taker's ability to obtain a substitute for the arrangement, and whether the arrangement is a direct MSP arrangement or an indirect MSP arrangement:

(f) any other information specified by the Bank.

Made at Wellington on [day month year].

Reserve Bank of New Zealand

Explanatory note

This standard comes into force on 1 December 2028.

The standard is issued under section 72 of the Deposit Takers Act 2023 and prescribes matters relating to the management of risk by a deposit taker and its policies and processes for business continuity planning as contemplated by section 85 of that Act.

The objective of the standard is to promote sound, effective, and efficient operational risk practices to enhance the operational resilience of deposit takers. It prescribes processes and controls to manage operational risks arising from, or in relation to, information and communication technology systems, arrangements with material service providers, and business continuity plans. A further objective is to mitigate the impact of operational risks that disrupt a deposit taker's critical operations.

Part 2 (relating to operational risk and critical operations) provides definitions of operational risk and critical operations. A deposit taker is required to identify the operations that are critical to its business and to document those operations. The Part sets out certain operations that, if a deposit taker undertakes them, are defined as critical for the deposit taker.

Each critical operation has a tolerance level set by the deposit taker consistent with its risk appetite statement made under the Deposit Takers (Risk Management) Standard 2027. The deposit taker is required to monitor its tolerance levels, and report any failure to the board.

Part 2 also requires a deposit taker keep a register of its critical operations and their associated tolerance levels.

Part 3 (relating to operation risk management frameworks) sets out the requirements for an operational risk framework that must be established and maintained by a deposit taker. For this purpose, the board and senior management must have the skills, experience, and knowledge to ensure that the deposit taker can manage operational risks effectively.

As part of the framework, a deposit taker must have an operational risk profile that includes an assessment of the impact of its business and strategic decisions on its operational resilience. A deposit taker is required to consider all operational risks to its business operations however they may arise and must design internal operational risk controls that are consistent with its risk appetite statement.

Part 3 also requires regular monitoring, review, and testing of a deposit taker's operational risk management processes and systems.

Part 4 (relating to information and communication technology risks) sets out how a deposit taker supports the security of its ICT systems and monitors its performance, requiring the deposit taker to identify and classify the elements of its systems based on criticality. The deposit taker must have an ICT systems policy to maintain that security. In addition, effective information security controls and information-sharing processes are required along with the consequent assurance processes.

This Part also provides what is to happen when a deposit taker has a material ICT systems incident, requiring notification to the Reserve Bank within a certain time frame.

Part 5 concerns risks related to material service providers. It provides a definition of who is a material service provider and sets out the scope of, and requirements for arrangements with, material service providers. The deposit taker is required to have a policy for service provider management that documents the identification, management, and mitigation of the operational risks associated with material service providers.

The Part also provides for the management of the ICT risks posed by a deposit taker's use of material service providers. It sets out the reporting requirements associated with material service providers. It is important to note that *Part 2* provides a requirement for a deposit taker to keep a register of its material service providers which must be updated regularly.

Part 6 (relating to business continuity plans) sets out how a deposit taker identifies, manages, and responds to an operational disruption event by way of its business continuity plan, and how the plan is tested and reviewed. It requires the deposit taker to give periodic assurances to the board and sets out how a business continuity plan would be notified.

Part 7 sets out the respective responsibilities of the board and senior management. The Part also provides for the responsibilities of a deposit taker when acting as group head. These

responsibilities include maintaining an appropriate operational risk management framework for the group and ensuring that subsidiaries have adequate business continuity plans.

This is secondary legislation issued under the authority of the Legislation Act 2019.	
Title	Deposit Takers (Operational Resilience) Standard 2027
Principal or amendment	Principal
Consolidated version	No
Empowering Act and provisions	Deposit Takers Act 2023 section 72
Replacement empowering Act and provisions	Not applicable
Maker name	Reserve Bank of New Zealand
Administering agency	Reserve Bank of New Zealand
Date made	[day month year]
Publication date	Click or tap to enter a date
Notification date	Click or tap to enter a date
Commencement date	1 December 2028
End date (when applicable)	Click or tap to enter a date
Consolidation as at date	Not applicable
Related instruments	Not applicable