Reserve Bank of New Zealand
Te Pūtea Matua

Deposit Takers (Operational Resilience) Standard 2027

Guidance Note

GN XX.1

Guidance Note version history

June 2026	Consultation draft	Relates to the exposure draft of the Operational Resilience Standard dated [June 2026]
[Day Month] 20XX	First issue date	Relates to Operational Resilience Standard version dated [2028]

Disclaimer

We produce a variety of publications and research about monetary policy, financial stability and related economic and financial issues. Most are available without charge as part of our public information service.

We have made every effort to ensure that information published in this Guidance Note is accurate and up to date. However, we take no responsibility and accept no liability arising from:

- errors or omissions
- the way in which any information is interpreted
- reliance upon any material.

We are not responsible for the contents or reliability of any linked websites and do not necessarily endorse the views expressed within them.

Privacy Policy - Reserve Bank of New Zealand - Te Pūtea Matua (rbnz.govt.nz)

Contents

Use and status of the Guidance

The purpose of this Guidance is to assist licensed deposit takers (or **deposit takers**) to interpret and comply with the Deposit Takers (Operational Resilience) Standard 2027 (the **Standard**). This recognises that the Standard deals with technical subject matter and there may be no case law or other external reference points to assist with its interpretation. Guidance will assist individual deposit takers with their own compliance and support a more consistent approach across the industry.

The Guidance assists by:

- outlining the context and purpose of the Standard. Technical content is better understood with awareness of the policy intent at the time it was drafted,
- outlining our preferred interpretation in relation to some clauses, where we (The Reserve Bank) have been made aware of differing interpretations by deposit takers, and
- providing examples of good practice in complying with the Standard.

To assist in using the Guidance:

- Terms that are defined in the Standard or the Deposit Takers Act 2023 (the **DTA**) are italicised in this Guidance and have the same meaning.
- The Guidance is designed to be read alongside the Standard. Sections of this Guidance have the same headings as sections of the Standard and Clause numbers are those from the Standard.
- In the event of any conflict between the text of the Standard and this Guidance, the Standard prevails. The Standard is secondary legislation made under the DTA, while the Guidance does not have formal status. The Guidance represents our view and is therefore an authoritative indicator of that view. However, ultimately, it is for a court to determine the correct interpretation of the Standard.
- The Reserve Bank will keep under constant review and update the Guidance. We may change our guidance or our interpretation of the Standard if we consider this appropriate. We do not do this lightly and will endeavour to notify deposit takers in advance if we are considering amending the content of the Guidance.
- This Guidance is not legal advice. We encourage deposit takers to seek their own professional advice, as it is their responsibility to determine their obligations and ensure that they comply with the requirements of the Standard.
- The Guidance relates to the version of the Standard as at [day month year].
- We welcome feedback on the Guidance at any time.

Part A: About this Standard

Overview

1. The Deposit Takers (Operational Resilience) Standard 2027 (the **Standard**) sets out requirements for deposit takers in the following areas to enable them to remain resilient through operational disruptions:

    - **operational risk management:** requirements to manage operational risk through identification and assessment of the deposit taker's operational risk profile, effective operational risk controls and reporting relating to operational risk incidents;
    - **information and communications technology (ICT):** requirements to manage risks arising from the use of ICT, including cyber risks;
    - **material service providers (MSP):** requirements to manage risks arising from the use of external service providers that provide critical operations to the deposit taker's business; and
    - **business continuity planning (BCP):** requirements to support the operational resilience of a deposit taker's critical operations during business disruptions, including through the development and use of BCP.

Context and purpose of the Operational Resilience Standard

2. The Standard sets out requirements to help ensure that deposit takers adequately manage their operational risks and remain resilient through operational disruptions. It aims to promote sound, effective and efficient operational risk practices that enhance the operational resilience of each deposit taker, which is important for maintaining operational continuity. The application of the Standard to the groups of deposit takers in the Reserve Bank's Proportionality Framework is outlined in Table 1 below.[1]

Table 1: Application of the Standard's requirements to deposit taker groups

Section	Group 1	Group 2	Group 3	Branches of overseas licensed deposit takers
Part 2: Operational risk and critical operations	✓	✓	✓	✓
Part 3: Operational risk management frameworks	✓	✓	✓	✓
	Some requirements do not apply to Group 3 deposit takers and branches of overseas licensed deposit takers			
Part 4: Management of ICT systems risks	✓	✓	✓	✓
	Some requirements do not apply to Group 3 deposit takers and branches of overseas licensed deposit takers			

[1] Refer to Proportionality Framework for developing standards under the Deposit Takers Act.

Section	Group 1	Group 2	Group 3	Branches of overseas licensed deposit takers
Part 5: Management of MSP risks	✓	✓	✓	✓
Part 6: BCPs	✓	✓	✓	✓
	Some requirements do not apply to Group 3 deposit takers and branches of overseas licensed deposit takers			
Part 7: Governance responsibilities	✓	✓	✓	✓

3. In addition to complying in different ways, some requirements do not apply to Group 3 deposit takers and branches of overseas licensed deposit takers. The aim of this is to simplify how Group 3 deposit takers and branches of overseas licensed deposit takers can comply with the Standard, commensurate with the size and nature of their business. This is discussed further in the section on proportionality below. We also highlight the areas where requirements do not apply to Group 3 deposit takers and branches of overseas licensed deposit takers in the applicable parts of this Guidance.

4. The Standard supports the Deposit Takers (Risk Management) Standard 2027 (the Risk Management Standard) by setting out more specific requirements for managing operational risks. The Risk Management Standard sets out the general approach and requirements relating to the identification and management of financial and operational risks. The Standard supports this objective by providing additional requirements relating to operational risk tolerances and mitigation, and response actions during operational disruptions.

Proportionality

5. The Standard sets out requirements relating to responsibilities, accountabilities, processes and practices, which the Reserve Bank expects to be clearly documented, updated and appropriately communicated by deposit takers to achieve the intended policy outcomes.

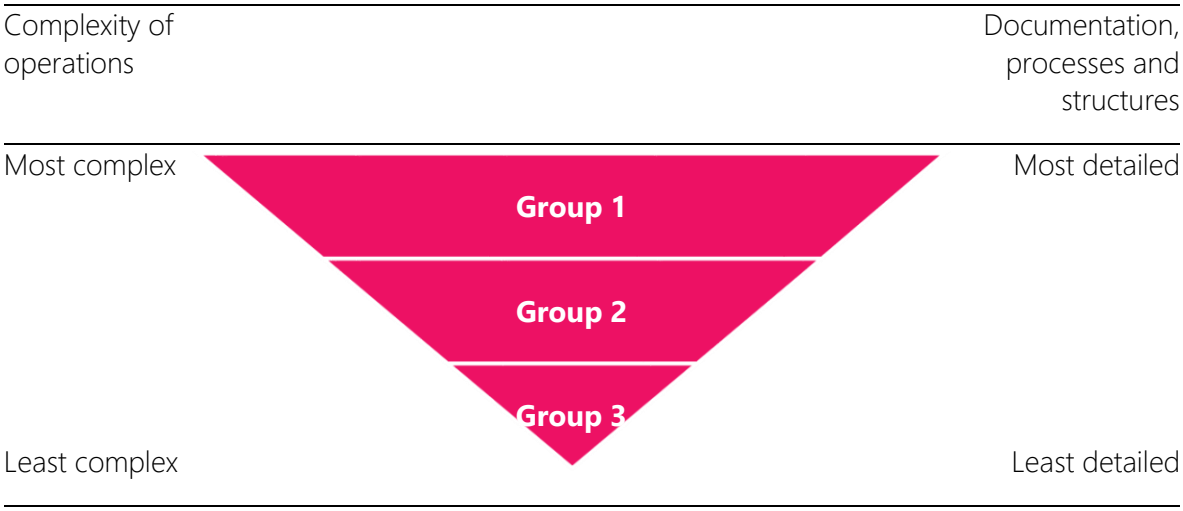
6. We expect a deposit taker to be able to demonstrate that its processes and policies are applied appropriately and work as intended in practice. We emphasise the importance of focusing on the outcomes in fulfilling the requirements as opposed to approaching compliance as a checkbox exercise. Doing so will allow a deposit taker to implement the requirements in a manner appropriate to the size and nature of their business.

7. In general, we expect larger deposit takers with typically more complex operations to have relatively greater specificity in documentation than smaller deposit takers with typically less complex operations (refer to Figure 1 below). Similarly, the processes and organisational structures of larger deposit takers with more complex operations will be more detailed compared to smaller deposit takers with less complex operations.

8. In particular, it is important to highlight that some of the "things to consider"-type illustrations we provide in this Guidance are deliberately fulsome in their nature. The intent of this is to

illustrate what we expect deposit takers to consider where it is relevant to their business operations and risk appetite, rather than being 'one size fits all' expectations for every deposit taker to take action to address everything listed in this Guidance.

Figure 1: Expected level of specificity of the documentation, processes and organisational structures by Group of deposit takers



9. Notwithstanding these general expectations on the relative level of detail and complexity of documentation, processes and organisational structures, we expect deposit takers to ensure these mechanisms are appropriate and robust on an ongoing basis. We also encourage deposit takers to go beyond minimum compliance when feasible to ensure that governance processes are fit for purpose for their business.

10. A deposit taker has discretion and flexibility in its adopted approach to documentation in complying with the requirements. For example, it may have a single document or multiple documents setting out information regarding all the required elements of the Standard. A deposit taker can also opt to cross-reference, where applicable, to minimise documentation duplication.

11. We recognise that the scale and nature of operational risks faced by deposit takers do not necessarily correspond to their relative business sizes, particularly given the accelerating digitalisation of financial services. For example, in some cases, a smaller deposit taker may operate through a fully digital model, resulting in a relatively more complex or interdependent operational environment than that of larger institutions.

12. We expect each deposit taker to prudently manage and build resilience against the operational risks inherent in its business model. This helps ensure continuity, adaptability, and recovery of critical operations commensurate with the size and nature of a deposit taker, as well as with the complexity of its business activities.

13. The guidance and examples described in the subsequent sections are not exhaustive.

Part B: Guidance on the Operational Resilience Standard

Part 1: General provisions

Objectives (Clause 3)

14. Clause 3 sets out the objectives of the Standard, including the risks that it seeks to mitigate, to enhance the operational resilience of deposit takers.

Interpretation (Clause 4)

15. Clause 4 provides definitions that are later used in the Standard. Consistent with section 20 of the Legislation Act 2019, words or expressions used in the Standard have the same meaning as in the DTA or referring legislation.

Application (Clause 5)

16. Clause 5 sets out how the Standard applies to different types of deposit takers. This includes that some requirements apply on a diminished basis for Group 3 deposit takers and overseas licensed deposit takers.

Approaches to applying and interpreting standard (Clause 6)

17. Clause 6 sets out that a deposit taker must determine the steps to meet the requirement in a way that a reasonable person would regard as both adequate for the requirement, and commensurate with the size and nature of the deposit taker's business

Group requirements (Clause 7)

18. Clause 7 sets out how a deposit taker that has subsidiaries, and is therefore the head of a group, is to comply with the requirements in respect of group operations. A deposit taker's conditions of licence may specify a particular entity or class of entities that the deposit taker must include or exclude in the group.

Reviews and testing programmes (Clause 8)

19. Clause 8 sets out the meaning of optimal frequency of reviews and testing if frequency is not explicitly stated. As noted in clause 8(2), unless otherwise stated in later clauses, a deposit taker may choose the optimal frequency or timeline for the review or testing that best fits their needs.

20. To provide some guidance across the specific required reviews listed in the Standard, Table 2 below sets out a summary overview of the reviews required within the Standard and their respective key points for a deposit taker to consider. Further details can be found in respective sections of this Guidance regarding each listed review.

Table 2: Reviews listed in the Standard

Standard clause	Review focus	Review frequency	Who conducts the review	Board required to see review results
12	Register of critical operations and MSPs	Annually (required)	Risk management function or business owner	No
15 / 17	Internal operational risk controls	At least once per 3 years (good practice)	Internal audit or another independent person (for example, consultants)	No – provided to senior management
	Operational risk management processes	At least once per 3 years (good practice)	Internal audit or another independent person (for example, consultants)	No
27 / 30	BCPs	At least once per 3 years or when there is a significant change in legal or organisational structure, business functions or business lines, or operational risk profile (good practice)	Internal audit or another independent person (for example, consultants)	Yes - if any substantive changes, both the board and the Bank to be notified

Note: where the board is not required to see review results, we expect that the board is notified that a review has been completed to ensure active oversight and challenge in practice. The timeframes in this table also align with expectations set out in the Risk Management Standard.

Part 2: Operational risk and critical operations

21. Part 2 of the Standard sets out the key definitions for the Standard relating to operational risk and critical operations. It requires deposit takers to identify their critical operations and set tolerance levels for managing them. Deposit takers are also required to maintain a register of their critical operations and MSPs.

Meaning of operational risk (Clause 9)

22. Clause 9 sets out the definition of operational risk as it is used in the Standard. It refers to the risk of loss resulting from either inadequate or failed internal processes, resources (including people), and systems, or an external event (an event originating outside of a deposit taker, and over which the entity has little or no direct control). This includes legal risk, but excludes strategic and reputational risk.

23. In managing its operational risks, a deposit taker is expected to manage a full range of risks, which may relate to the following (but not be limited to):

    23.1. change management,

    23.2. compliance,

    23.3. data,

    23.4. legal,

    23.5. regulations, and

    23.6. technology.

24. A deposit taker is responsible for identifying and assessing the operational risks it faces, and for determining what risks are material to its business. Operational risks can be interrelated and overlapping. We expect deposit takers to consider these risks holistically. Certain events can heighten or amplify risks and increase their materiality. For example, indirect risks such as geopolitical risks may result in increased cyber risks, or direct risks such as natural disasters which can directly impact a deposit taker's ability to maintain its critical operations.

25. We expect a deposit taker to clearly set out and document the underlying criteria used to determine the materiality of operational risks it faces. We expect the approach taken here to be consistent with Subpart 2 of the Risk Management Standard Guidance. Subpart 2 of the Risk Management Standard Guidance discusses that the criteria or factors used for determining material risks are expected to be clearly documented in the Risk Management Strategy (including quantitative and qualitative factors such as impact on business objectives, protection of customer interest, entity reputation and financial and operational stability).

Meaning and identification of critical operations (Clause 10)

26. Clause 10 defines critical operations, and this definition is used in other requirements of this Standard – that is, to define which operations provided by a deposit taker are subject to certain requirements. The definition includes operations that are performed by deposit takers in-house and those that are provided by external service providers.

27. Clause 10(1) requires deposit takers to identify which operations they undertake that meet the definition. Clause 10(3) sets out a non-exhaustive list of processes that must be defined as critical operations, where they exist.

28. In identifying critical operations, we expect a deposit taker to conduct a robust assessment of the implications if and when an operation is disrupted. At a minimum, we expect this assessment to detail if the disruption of the operation would have:

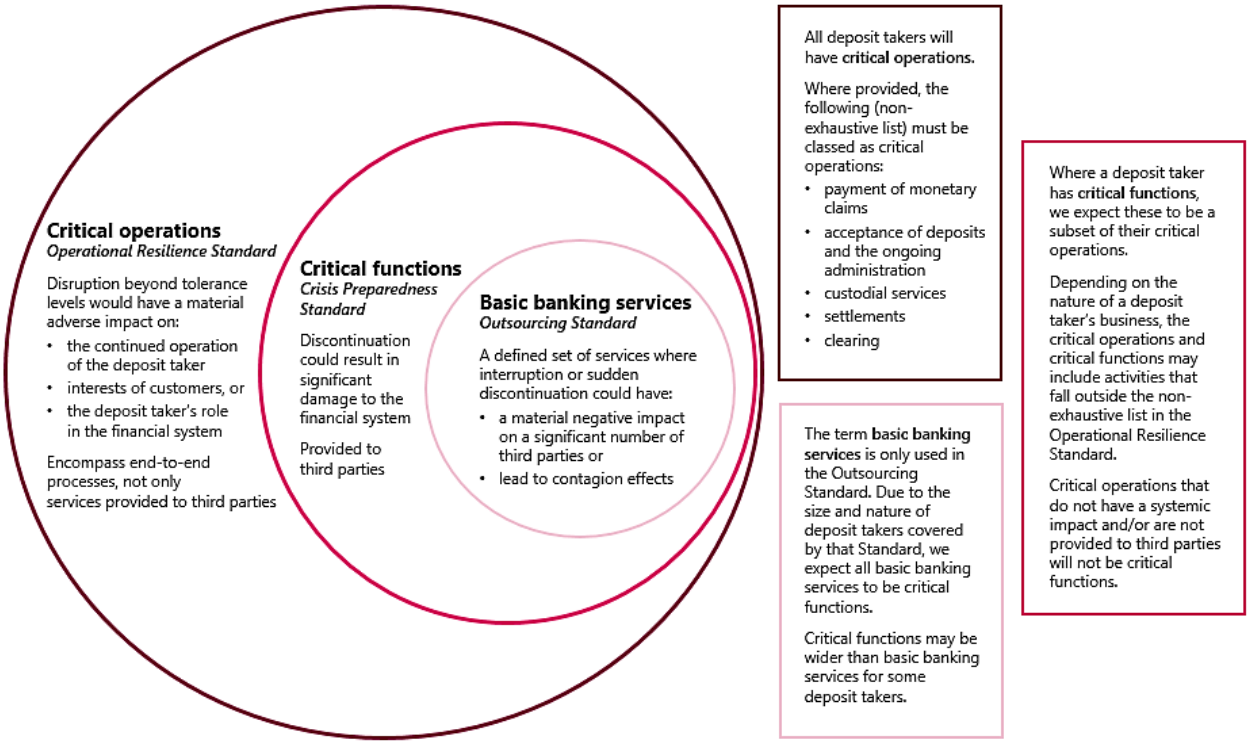
    28.1. direct or indirect material adverse impacts on depositors or other customers in their ability to access their information and conduct business with the deposit taker – such as the ability to receive funds, pay or transfer funds, or withdraw funds, among others;

    28.2. direct or indirect material adverse impacts on the deposit taker, in terms of the deposit taker's financial position, public reputation and credibility, and ability to comply with its prudential and legal obligations, among others; and

28.3. direct or indirect material adverse impacts on other entities in New Zealand within and outside of the financial sector that have ties with the deposit taker, in terms of the entities' financial position, public reputation and credibility, and ability to comply with their prudential and legal obligations, among others.

29. The Deposit Takers (Outsourcing) Standard 2027 (the Outsourcing Standard) uses similar concepts to critical operations. Figure 2 below clarifies the relationship between critical operations and critical functions, and between critical operations and basic banking services.

Figure 2: Relationship between critical operations and critical functions [*critical functions as proposed in the crisis management consultation documents*]



Tolerance levels for critical operations (Clause 11)

30. Clause 11 requires a deposit taker to establish a tolerance level for each of its critical operations. This is the limit within which the deposit taker can accept an operational disruption. Establishing tolerance levels for disruption sets the parameters to allow deposit takers to put in place the controls to allow these tolerance levels to be met.

31. Clause 11(2)(b) sets out some metrics that a deposit taker must establish when setting tolerance levels for disruptions to its critical operations. Table 3 below describes these metrics further. We expect that the criteria for how tolerance levels are set to be clearly documented and updated. This means that a deposit taker considers it a tolerance breach if the disruption results in impacts that fall outside the defined thresholds.

Table 3: Metrics that must be considered in setting tolerance levels for critical operations

Metric	Description
Time or duration	Maximum period of disruption to a critical operation that a deposit taker can tolerate.
Information loss	Maximum amount of data or information lost that a deposit taker can tolerate. We expect deposit takers to consider the sensitivity of information and the ability of the deposit taker to accurately reconstruct the lost information or recover them from back-up storage.
Service level	Minimum level of service that a deposit taker can tolerate, which we expect can be gauged by the volume and value of transactions a critical operation supports.

32. In setting out the tolerance levels, a deposit taker is encouraged to consider the maximum number of times a critical operation is disrupted within a period that it can tolerate. This will help ensure that cumulative impacts of several events impacting a critical operation in a specified period is considered in the assessment, in addition to the impact of a single event.

Register of critical operations and material service providers (Clause 12)

33. Clause 12 requires a deposit taker to establish and maintain a register to record both its critical operations and MSPs. The register is designed to ensure that there is a single record of all the deposit taker's critical operations and MSPs. The information that a deposit taker must include in the register for its MSPs is set out in Schedule 1 of the Standard.

34. Clause 12(3) requires a deposit taker to use the template provided by the Reserve Bank which is available on the Reserve Bank's website.

35. The template for the register includes information requirements to ensure compliance across both the Operational Resilience Standard and the Outsourcing Standard (for deposit takers where this standard applies, the Outsourcing Standard applies to deposit takers who are identified as a Group 1 deposit taker for the purpose of that Standard). The register will be used to provide a single source of information on critical operations and MSP arrangements, as required by the Operational Resilience and Outsourcing Standards. This information will be used to support supervision of both standards. Most requirements are contained in the Standard and outlined in Schedule 1. Part 6 of the Outsourcing Standard requires additional information to also be provided by deposit takers who are required to comply with that standard.

36. The register is intended to support deposit takers with BCPs, and it provides a single record to support the Reserve Bank's supervision of BCP and MSP requirements.

37. In the context of fostering operational resilience, it is important for the Reserve Bank to understand how financial service providers identify, manage and mitigate the associated operational risk. These requirements emphasise the importance of appropriate controls and processes being in place to adequately oversee and proactively manage the risks faced by deposit takers arising from the use of MSPs.

38. Cause 12(4)(a) requires a deposit taker to regularly review and update the register at least once in a 12-month period. Clauses 12(4)(b) and 12(4)(c) require a deposit taker to enter the details of any new MSP into the register and document any material changes to existing arrangements.

39. Clause 12(2) requires a deposit taker to provide the register to the Reserve Bank when it enters into a new arrangement with a material service provider or on request by the Reserve Bank. This is intended to align with the reporting requirements outlined in clause 26, where a deposit taker is required to notify the Reserve Bank as soon as is practicable. See clause 26 and the corresponding guidance for further detail.

Part 3: Operational risk management frameworks

40. Part 3 of the Standard sets out requirements relating to establishing and maintaining operational risk management frameworks. They are intended to ensure a deposit taker has a clear understanding of their operational risks, so that these risks are effectively managed to enable operational resilience.

Operational risk management frameworks (Clause 13)

41. Clause 13 requires a deposit taker to establish and maintain an operational risk management framework. This requirement is intended to ensure that deposit takers put in place a framework to manage operational risks effectively in order to maintain their operational resilience.

42. Clause 13(4) requires a deposit taker to have an operational risk management framework that is consistent with the Risk Management Standard. An operational risk management framework is a subset of a risk management framework, which as per the Risk Management Standard is the totality of systems, structures, policies, processes and people within an institution that identify, measure, evaluate, monitor, report on and control or mitigate all internal and external sources of material risks.

43. Part 2 of the Risk Management Standard and the accompanying Guidance document set out further details and requirements for a deposit taker's risk management framework, including both the risk management strategy and risk appetite statement.

44. The operational risk management framework is expected to include objectives relating to risk identification, risk assessment, and risk mitigation, as well as monitoring, review, communication, and engagement (refer to Figure 3 below). The intent is that the objectives of the frameworks reinforce each other, with consistent and informative communication and engagement with relevant staff on operational risks.

45. We expect a deposit taker to design strategies, policies, and processes to pursue the objectives of the framework. The underlying strategies, policies, and processes are expected to be clear on their scope and criteria, where relevant, and to appropriately consider the business, economic, and technological context in which the deposit taker operates.

46. The approach taken by a deposit taker to determine objectives may also include such considerations as concentration risk and substitutability. With this inverse relationship, concentration risk is high when there is insufficient substitutability, and vice versa. For example, a deposit taker would be expected to sufficiently consider the level of substitutability

it has regarding its ability to replace suppliers, services or assets without incurring material costs or operational disruptions.

Figure 3: An example of an operational risk management framework

Operational risk profile (Clause 14)

47. Clause 14 requires a deposit taker to establish and maintain an assessment of its operational risk profile. Effective operational risk management requires a sound understanding of the deposit taker's operational risk profile on an ongoing basis, and how its risk profile is changing with the circumstances in which it operates. The absence of such an assessment limits the ability of a deposit taker to adequately and effectively manage its operational risks on an ongoing basis.

48. We expect the assessment process to be consistent with, and proportionate to, the deposit taker's risk appetite statement which defines the level of risk it is willing to assume or tolerate to achieve its strategic objectives (refer to Part 2 of the Risk Management Standard and its accompanying Guidance document for further information).

49. A deposit taker is expected to detail the assessment considerations and process in its operational risk management framework. Table 4 outlines a list of areas that a deposit taker could consider in assessing its operational risk profile.

Table 4: Risk profile assessment areas

Area	Description
Context	Economic conditions, geopolitical risks, technology developments, sectoral developments and operational risk factors that affect or can affect the operational resilience of the deposit taker.
Critical operations	Register of critical operations, the considerations or reasons in identifying certain operations as critical operations and the processes and resources needed to deliver critical operations (including people, technology,

Area	Description
	information, facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls).
Risk information systems	Register of internal and external operational risks that have been identified and the risk analysis conducted by the deposit taker, particularly the causes of these risks. Analysis of the impact of the deposit taker's business and strategic decisions on its operational risk profile and operational resilience, including in the implementation of new products and services.
Controls	Register of controls to mitigate operational risks, and records of the results of assessments or tests of these controls (particularly the gaps and weaknesses).
Risk appetite	Alignment of operational risk management with the deposit taker's risk appetite.
Actions	Records of remedial measures undertaken to mitigate or lower internal and external operational risks, especially when these risks are assessed by the deposit taker to exceed the risk appetite.

50. Clause 14(1)(c) requires Group 1 and 2 deposit takers to include an assessment of the impact of their business and strategic decisions on its operational resilience. As a matter of good practice, Group 3 could consider such an assessment to strengthen their assessment of their operational risk profile.

51. We expect the assessment to consider changes in the deposit taker's strategic direction as well as changes in business, economic and technological context where the deposit taker operates.

52. The assessment of the operational risk profile could use scenario analyses to consider extremely challenging events to identify gaps in the deposit taker's operational risk management framework.

53. In maintaining their operational risk profile, we expect that the profile will be reviewed on a regular basis commensurate with the size and nature of the deposit takers business. A deposit taker has the flexibility in determining the regularity of its assessment. The frequency is expected to support the deposit taker's ability to demonstrate to the Reserve Bank, if requested, that its current assessment of its risk profile remains appropriate.

Operational risk practices and internal controls (Clause 15)

54. Clause 15 sets out what a deposit taker is required to do to manage its operational resilience. It must consider all operational risks to its business operations however they may arise. We expect deposit takers to take a holistic approach to managing their operational risks, commensurate with the size and nature of their business. Senior management has

responsibility for implementing operational risk management across the end-to-end process for all business operations (as outlined in clause 34).

55. Clause 15(1)(b) requires a deposit taker to have processes and controls in place to manage the operational risks. We expect these processes and controls to be designed, implemented, embedded, monitored, reviewed and tested to mitigate any current and incipient operational risks in line with its set risk appetite and meet its compliance obligations. The frequency of review is intended to be commensurate with the size, nature and complexity of risks being controlled.

56. Clause 15(2) requires a deposit taker to design and maintain internal operational risk controls to align with its risk appetite and support its capability to comply with its obligations under the Risk Management Standard. We expect internal controls to be designed in a way that gives the deposit taker the confidence to provide assurance to the Reserve Bank that it is efficiently and effectively mitigating its operational risks, particularly to its critical operations, on an ongoing basis. Details regarding internal control reviews are provided under clause 17.

57. Subpart 4 of the Guidance on the Risk Management Standard highlights having a strong internal control framework is part of sound corporate governance and risk management. In establishing and maintaining an effectively controlled and tested operating environment with internal controls in place, we expect a deposit taker to consider its own risk profile and take a forward-looking view.

58. In managing operational risk incidents, a deposit taker may consider the steps outlined in Table 5. A deposit taker is expected to have adequate capability, capacity and processes to credibly support its internal controls.

Table 5: Managing operational risk incidents

Action/Stage	Description
Detection and identification	Ascertain the occurrence of operational risk incidents and identify the key characteristics of the incidents.
Escalation	Escalate operational risk incidents, if necessary, based on internally defined thresholds, for further and more detailed assessment.
Response, containment and remedial measures	Respond to, contain the impact of and remediate the operational risk incidents.
Review	Analyse and review the nature of incident, especially the root cause, the impact and the actions undertaken to respond to the incident and utilise the findings to continuously improve the internal controls.

Material operational risk incidents (Clause 16)

59. Clause 16 sets out the incident reporting requirements for a deposit taker when a material operational risk incident happens – this being an operational risk incident that the deposit taker determines to be likely to have a material financial impact or a material impact on the

ability of the deposit taker to maintain its critical operations. This requirement ensures that the Reserve Bank is promptly informed of any material operational risk incident affecting a New Zealand deposit taker, enabling effective monitoring of how the incident is being managed and how the associated risks are being contained to protect the deposit taker's ongoing operations.

60. We expect the materiality threshold, which relates to the deposit taker's financial position and its ability to maintain critical operations, to be applied on a case-by-case basis. A deposit taker has flexibility to apply this threshold given its own circumstances when determining whether an incident is material.

61. A deposit taker is expected to consider applying either quantitative and qualitative criteria (or both) when assessing if an incident meets the materiality threshold. Where the impact of an incident is uncertain, the deposit taker is expected to make a reasonable assessment based on the available information at the time and update the assessment as further information becomes available.

62. In assessing materiality, a deposit taker could consider the following factors:

    62.1. whether the incident has affected, or could reasonably affect:

        62.1.1. the availability, performance or integrity of a critical operation,

        62.1.2. the customers' ability to access banking services, funds, or support channels,

    62.2. the number or proportion of customers affected, including any impact on vulnerable or high-priority customer groups,

    62.3. the number, value, timeliness, accuracy or integrity of transactions, payments, settlements or customer instructions,

    62.4. the duration of the incident, including service degradation, reduced capacity, recurring disruption or reliance on manual workarounds,

    62.5. the confidentiality, integrity or availability of customer, financial, operational, regulatory or security data,

    62.6. actual or suspected malicious cyber activity, unauthorised access, credential compromise, malware, ransomware, data compromise or loss of system controls,

    62.7. the deposit taker's financial position including direct loss, fraud loss or remediation costs,

    62.8. whether a material third party, material service provider, cloud provider, payment provider, telecommunications provider or other dependency is supporting a critical operation,

    62.9. the need to notify another regulator, government agency, law enforcement body, payment system operator, privacy authority or oversea authority,

    62.10. reputational impact, media attention, public confidence or market confidence, or

62.11. whether the incident forms part of a pattern of repeat incidents, recurring control weaknesses, unresolved remediation or known vulnerabilities.

63. Clause 16(2) requires a deposit taker to notify the Reserve Bank of an operational risk incident as soon as is practicable and, in any case, no later than 72 hours after the deposit taker has become aware of it. We expect earlier notification and engagement to support supervisory engagement. A deposit taker may submit an initial report that is incomplete if certain information is not yet available within the first 72 hours and provide the missing information in subsequent reports to the Reserve Bank. It may also amend any details previously supplied to the Reserve Bank if those details are later found to be incorrect or inaccurate. The 72-hour period starts from the time the incident is determined to be material.

64. The Reserve Bank may also request additional information from the deposit taker regarding the incident reported as a part of ongoing supervisory engagement relating to the incident.

Reviews of operational risk management processes and systems (Clause 17)

65. Clause 17 sets out review requirements for a deposit taker's internal operational risk control and its operational risk management processes and systems. In reviewing the effectiveness of the internal controls, a deposit taker could consider:

    65.1. having clear and consistent testing criteria, which could include the detection rate and success rate in identifying, containing and remediating the operational risk incidents,

    65.2. examining the design and operational effectiveness of the controls separately,

    65.3. testing the controls' responsiveness to material and non-material risks,

    65.4. capturing how internal controls are affected or could be affected by controls of the deposit taker's service providers, and

    65.5. recording the results and any changes in the environment or business strategies that could impact the effectiveness of internal controls moving forward.

66. Clause 17(1) requires a deposit taker to regularly monitor, review, and test its internal controls. As good practice, we encourage internal control reviews to be conducted at least once every 3 years, with more regular periodic reviews conducted as required considering an individual deposit taker's business needs, consistent with clauses 6 and 8.

67. A deposit taker also has flexibility in determining who conducts periodic risk-based reviews. For example, it may be conducted by an internal or external reviewer provided that the reviewer is qualified and sufficiently operationally independent.

68. Clause 17(2) requires a deposit taker to provide testing results to its senior management and the issues identified during testing must be addressed in a timely way. We expect senior management to report results to the board when material issues are identified. A deposit taker is expected to address the weaknesses in the internal controls that were identified in the review process in a timely manner.

Part 4: Management of ICT systems risks

69. Part 4 sets out requirements to support the effective management of risks to a deposit taker's information and communication technology (ICT) systems. These requirements specify the processes, controls, and tolerance levels that must be in place to support the robustness and security of ICT systems and the continuity of critical operations. It also outlines the key features of an ICT systems policy and a deposit taker's obligations for reporting ICT systems incidents.

Managing information and communication technology risks (Clause 18)

70. Clause 18 sets out requirements to support a deposit taker's ability to manage risks to the security of its ICT systems. It requires a deposit taker to establish and maintain processes, controls, and tolerance levels that are appropriate for its operational risk profile to support the security of ICT systems and monitor the performance of those systems. Consistent with clause 8, a deposit taker is required to document and regularly review these processes, controls, and tolerance levels.

71. In the context of clause 18, we expect this to include, but not be limited to, establishing processes to control or manage:

    71.1. system accounts, access privileges, interdependencies across functions and roster of key personnel that support ICT systems;

    71.2. security controls and monitoring;

    71.3. ICT systems' vulnerabilities assessments, including security controls effectiveness tests and assurances;

    71.4. detection of anomalous or malicious activities, reporting of these activities and analysis of the information collected; and

    71.5. responses to and recovery from breaches and anomalous or malicious incidents.

72. Regarding interdependencies, a deposit taker is expected to have a clear understanding on how ICT systems support multiple functions across the organisation, and how disruptions, access issues, or system failures may affect functions beyond ICT systems. This includes dependencies that are not limited to system accounts or access privileges, such as reliance on shared platforms, data flows between functions, or operational processes that depend on the same ICT systems. Examples could include:

    72.1. shared ICT systems across business functions;

    72.2. ICT systems supporting operational processes outside ICT systems; and

    72.3. dependencies between front-office and support functions.

73. In establishing these processes, clause 18(2)(a) requires a deposit taker to identify and classify its ICT systems based on criticality. We expect a deposit taker to take a risk-based approach when establishing its criteria for classification. Criticality may be based on financial or non-financial scale of impact, recoverability, and substitutability. Elements could include:

    73.1. underlying infrastructure;

    73.2. related processes;

73.3. information assets;

73.4. internal and customer-facing applications;

73.5. ICT systems services and dependencies, including cloud services; and

73.6. interconnection points and interfaces (for example, application programming interfaces).

74. We expect tolerance levels for ICT systems to be integrated with the deposit taker's processes to detect, monitor, respond to and recover from anomalous or malicious incidents affecting those ICT systems.

75. A deposit taker has the flexibility to determine the criticality of its ICT systems, having regard to the deposit taker's size, complexity, business model, and operating environment. Assessing criticality of ICT systems is expected to take into account both direct or indirect support for operational processes.

76. Clause 18(2)(b) requires a deposit taker to establish processes and security controls to prevent, detect, monitor, respond to, and recover from disruptions affecting its ICT systems. The intent of these processes and security controls is to support the security, resilience, and reliable operation of ICT systems, and mitigate impact of ICT systems incidents on critical operations.

77. These processes and controls may focus on whether the failure, degradation, or compromise of the ICT systems would reasonably be expected to:

77.1. prevent, delay, or otherwise impair the delivery of the critical operation;

77.2. undermine the availability, integrity, confidentiality, or timeliness of information required to deliver the critical operation;

77.3. weaken the effectiveness of controls, safeguards, or recovery arrangements that are relied upon to maintain the delivery of the critical operation; or

77.4. affect other ICT systems that support the delivery of the critical operation, including through shared services, common infrastructure, or dependencies.

78. A deposit taker could consider Part B of our *Guidance on Cyber Resilience* in the context of ICT systems in building capability and ensuring that the ICT systems are secure.

79. Box 1 below discusses ICT systems risks that may arise from the use of artificial intelligence (AI).

Box 1. Artificial Intelligence and the operational resilience of critical operations

Where AI systems, models, tools or AI-enabled third-party services support or materially affect critical operations, we expect a deposit taker to assess the resilience implication of that AI dependency. This could include consideration of whether an AI failure, misuse, bias, lack of explainability, model drift, poor data quality, cyber compromise or third-party failure could impair the continued delivery of the critical operation within approved impact tolerances (clause 11).

We expect these AI dependencies to be subject to appropriate governance, monitoring, human oversight, fallback arrangements, incident response procedures and scenario testing. The assessment could cover availability of the underlying technology, reliability, integrity and explainability of the AI-generated outputs where these may affect customers, operations, decision making or regulatory obligations.

We also expect deposit takers to consider external risks arising from the use of AI by malicious actors, where these could affect the continued delivery of critical operations. This could include consideration of whether AI-powered phishing, social engineering, fraud, credential compromise, malware development, cyber reconnaissance, deepfakes, or other forms of malicious activity could increase the frequency, scale, speed or sophistication of attacks against the deposit taker or its service providers. Where relevant, we expect deposit takers to assess existing controls, response arrangements and recovery capabilities remain sufficient to maintain critical operations within approved impact tolerances.

ICT systems policy (Clause 19)

80. Clause 19(1) requires a deposit taker to have an ICT systems policy to maintain the security of its ICT systems and protect its critical operations. A proportionate and fit-for-purpose ICT systems policy (or equivalent) supports consistent, effective, and appropriate management of security risks to a deposit taker's ICT systems.

81. Clauses 19(2)(a) and 19(2)(b) require that the ICT systems policy is consistent with the deposit taker's operational risk profile, and that the deposit taker's ICT systems are capable of adequately responding on an ongoing basis to system failures and threats.

82. We expect the ICT systems policy to be documented and to clearly articulate the deposit taker's objectives, principles, and expectations for resourcing necessary to maintain secure ICT systems. While the policy would not set specific resourcing decisions, it is expected to establish the standards and requirements that inform decisions on funding, staffing, access to appropriate skill sets and control environment capability needed to prevent, detect and respond to ICT systems risks.

83. We expect the policy to include, but not be limited to:

    83.1. policy objectives,

    83.2. responsibilities, including the responsibility of the board and senior managers,

    83.3. risk appetite and risk tolerance levels,

    83.4. resilience targets and implementation plan,

    83.5. threat and vulnerability information that must be reported to the board or senior managers, and

    83.6. roles responsible for ensuring the security of ICT systems, their responsibilities, and the processes for vetting these personnel.

84. Regarding the *roles responsible for ensuring the security of ICT systems* mentioned in paragraph 83.6, these are bodies or individuals that would typically have decision-making, approval, oversight and operations responsibilities. These could include the following (or their equivalents):

84.1. chief information security, information technology or ICT systems officer;

84.2. information security, information technology or ICT systems oversight committee;

84.3. board and/or management risk management committee;

84.4. board audit committee;

84.5. executive management committee; and

84.6. information security, information technology, or ICT systems operations administrator.

85. A deposit taker could consider Section A1 of our *Guidance on Cyber Resilience* in the context of ICT systems in setting out responsibilities.

86. Clause 19(2)(c) requires that the policy provides for an ICT systems incident management framework and escalation process. In developing escalation processes, a deposit taker could consider:

86.1. the types of risks to ICT systems and incidents that require escalation, including thresholds for escalation to senior management and the board;

86.2. information that must be included in the escalation report;

86.3. prioritisation classification and criteria;

86.4. roles and responsibilities for initiating, managing, and approving escalation;

86.5. timeframes for escalation, having regard to the potential impact on critical operations and the interests of depositors or other customers;

86.6. how escalation processes interact with incident response, recovery, and communication arrangements; and

86.7. reviews of previously escalated incidents to assess whether the process is operating as intended and to identify opportunities for improvement.

87. In developing its ICT systems incident management framework, a deposit taker could include the following elements:

87.1. structured lifecycle: defined stages for managing ICT systems incidents, including detection, identification, logging, categorisation, impact-based restoration prioritisation, and closure;

87.2. restoration processes: processes for restoring affected parts of ICT systems, including the use of workarounds or system recovery to return services to defined normal or service levels;

87.3. feedback and continuous improvement: processes, such as post-incident reviews, that use incident data to identify root causes and mitigate the risk of recurrence; and

87.4. accountability: defined accountability arrangements, identifying specific roles and escalation authorities responsible for the command and control of ICT systems incident response.

88. In general, a deposit taker could consider Section A2 of our *Guidance on Cyber Resilience* in the context of ICT systems in developing its ICT systems policy.

89. We expect the ICT systems policy to be reviewed on a regular basis commensurate with the size and nature of the deposit takers business.

Assurance and information-sharing processes (Clause 20)

90. Clause 20 sets out requirements to support information security. These requirements are structured around three key elements: information sharing processes, information security controls, and assurance processes. The intent is to ensure that risks are appropriately identified and managed, and sensitive information is protected from unauthorised access or misuse.

91. Figure 4 provides a framework on the linkage between information access and sharing process, controls, assurance and assurance assessments. This is discussed further below.

Figure 4: Information access and sharing process, information security controls, and assurance

Information sharing process

92. Clauses 20(1) and 20(3) set out the requirements relating to information sharing processes. To help support their effectiveness, we expect these processes to be clearly documented, kept up to date, appropriately communicated, and effectively enforced. The intent of this is to ensure that critical information is shared only with persons authorised to receive it. As a matter of good practice, the processes could also outline how relevant information is identified and routed to the appropriate recipients.

93. We expect a deposit taker to clearly identify the modalities and the manner that it considers appropriate in sharing or transferring information. For example:

    93.1. A deposit taker may utilise information security classification markings to set out which information and how this information can be shared, and/or level of encryption for the different types of information.

    93.2. Methods of information sharing may include distribution of physical documents and use of portable devices (such as portable computers, mobile phones, hard drives or flash drives), electronic or digital sharing tools (such as emails, cloud folders and servers or wireless personal area networks) and data extraction tools (such as statistical or application development software through accessible network connections, application programming interfaces or web scraping).

94. We expect a deposit taker to clearly define what it considers an information breach or leakage. Information breach or leakage refers to unauthorised removal, copying, distribution or disclosure of information, particularly where the information is sensitive, and results in loss of information confidentiality or other unauthorised exposure of information.

95. A deposit taker could consider Part C of our *Guidance on Cyber Resilience* in the context of ICT systems in developing its information sharing practices.

Information security controls

96. Clause 20(1) sets out the requirements relating to information security controls. We expect a deposit taker to document its information security controls to provide clarity on their design and intended operation, support consistent implementation, and facilitate effective oversight. Table 6 outlines some examples of operational areas that deposit takers could consider having information security controls.

Table 6: Examples of operational areas that would benefit from information security controls

Information security control area	Description
Change management	Processes that support the management of changes to a deposit taker's personnel and information systems in a way that appropriately considers information security and incorporate appropriate controls, including identifying and managing routine and urgent changes to systems.
Configuration management	Processes that support the configuration of information systems in accordance with approved configuration standards and security baselines. Configurations are expected to be documented, reviewed periodically, and reassessed following a material system change to ensure they remain appropriate and aligned with the deposit taker's ICT systems requirements.
Deployment and environment management	Processes that support secure environment for developing and testing functionalities, including the underlying processes, and the subsequent deployment of these functionalities are expected to consider the deposit taker's information security and incorporate appropriate information security controls.
Access management controls	Processes for granting information access authorisations to personnel (such as multi factor authentication and session logging for privilege access), software and hardware, including those provided by vendors. These processes are expected to incorporate appropriate information security controls and may also include authorisation models such as role-based access control (RBAC), policy-based access control (PBAC) or attribute-based access controls (ABAC).
Hardware and software asset controls	Processes for managing and protecting information contained in the deposit taker's hardware and software assets, including those provided by vendors. These processes are expected to incorporate appropriate authorisation and control mechanisms to prevent information security compromise throughout the asset lifecycle. The lifecycle includes initial procurement, deployment, operation, maintenance (including the application of patches and updates), and eventual decommissioning or disposal.

Information security control area	Description
Network design	Processes that support authorised network traffic flows and incorporate appropriate segregation and protective controls to reduce the impact of information security compromises. Network segmentation and defined perimeters are based on trust level or function. Relevant controls ensure traffic flows are known, controlled, and supportable.
Vulnerability management controls	Processes for identifying, assessing, prioritising, and addressing information security vulnerabilities in a timely manner, including where new vulnerabilities and threats are discovered, to support timely remediation and reduce the likelihood of compromise.
Patch management controls	Processes for assessing, testing (where appropriate), and timely application of patches and other updates addressing known vulnerabilities. These processes are expected to apply across the deposit taker's hardware and software assets, including relevant vendor-provided components, and cover patch updates embedded within ICT systems, as well as the timeliness and sequencing of patch deployment.
Service level management mechanisms	Processes for monitoring and managing of service performance, aligning information security outcomes with business objectives, including through clear service requirements, service levels, and oversight of performance against those expectations. These include identifying and monitoring service requirements and service levels for relevant information systems and monitoring of performance against agreed service levels, and reporting that supports, informing remediation actions where needed.
Monitoring controls	Processes that support the timely detection of information security compromises through appropriate logging, alerting, and analysis of relevant security events, including the identification of abnormal or malicious behaviour. This may include the use of security logs and event data sent to a central capability for correlation, analysis, and alerting.
Response controls	Processes for managing information security incidents, including investigation, containment, remediation, and recovery, and for incorporating feedback mechanisms (such as post-incident reviews) to address control deficiencies and reduce the likelihood of recurrence. These may include processes to investigate, contain, eradicate, and recover from security incidents, address control deficiencies identified through incidents, and support post-incident feedback and improvement.
Capacity and performance management controls	Processes that support the availability of information security services by monitoring current performance and projected demand, to help ensure that availability is not compromised by current or expected business volumes. These may include monitoring key performance indicators

Information security control area	Description
	(such as capacity, utilisation, and latency) for systems supporting information security and assessing future demand to inform scaling and resilience planning.
Cryptography management	Processes for managing cryptographic keys, certificates and related cryptographic dependencies throughout their lifecycle, including key generation, exchange, storage, rotation and destruction, and certificate issuance, renewal, revocation, expiry monitoring and inventory management. This could include the ability to identify, assess and replace cryptographic mechanisms where vulnerabilities emerge or contemporary cryptographic standards change.
Service provider management controls	Processes that support assurance that a deposit taker's information security requirements are met where services, systems, or components are provided by service providers, including through appropriate oversight, monitoring of service levels, and management of risks arising from those arrangements. These may include monitoring service providers, service level agreements, and associated risks; vetting relevant service provider personnel where appropriate; and ensuring that vendor-provided software and hardware are captured within access and asset control processes.

97. The information security controls could also include the following mechanisms:

    97.1. information classification based on criticality, access authorisations of personnel, and processes when there are changes to these authorisations (for example, when personnel with ICT responsibilities leave the deposit taker or move to another unit within the deposit taker);

    97.2. layered security controls (defence-in-depth) to protect its information systems, such that if one control fails, other controls could limit the impact of an incident, including firewalls, endpoint detection and response systems, network access controls, malware protection, encryption and security monitoring tools;

    97.3. adversarial testing, including red team exercises or where appropriate threat-led red team exercises, to validate the effectiveness of information security controls against plausible attack scenarios, with an option to extend the scope to purple team testing where the objective includes improving detection and response capability;

    97.4. allocation of responsibility and accountability for the information security; and

    97.5. measures that help ensure that personnel with responsibility and accountability for the information security have the capacity to perform their duties.

98. Deposit takers could also refer to Part 3 of the Risk Management Standard and the accompanying Guidance for requirements relating to information and data management.

Information security controls assurance processes

99. Clause 20(2) sets out the requirements relating to information security controls assurance processes. We expect a deposit takers information security control assurance process to be clearly documented and provide information on the effectiveness of the information security controls at each stage of the life-cycle of the information asset. This includes the purchase and development, maintenance and decommissioning of the information asset.

100. The assurance process is expected to be conducted on a periodic and risk-based basis, and following material changes or incidents, as appropriate. The intent of assurance reports is to inform risk management, remediation actions, and report to senior management and the board, where appropriate.

101. As a matter of good practice, a deposit taker could periodically assess whether the assurance process remains fit for purpose. For example, this may include assessing whether the scope remains aligned with risks, whether assurance methods remain appropriate, and whether management can reasonably rely on the assurance produced.

102. Clause 20(2) does not apply to Group 3 deposit takers and overseas licensed deposit takers.

Material ICT systems incidents and control weaknesses (Clause 21)

103. Clause 21 requires a deposit taker to notify the Reserve 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 it. We expect earlier notification and engagement to support supervisory engagement. ICT systems incidents are a subset of the risks required to be reported under clause 16. The requirements in clauses 16 and 21 support the Reserve Bank's monitoring of how material operational risk incidents, including ICT systems incidents, are managed and contained.

104. Aligned with clause 16, a deposit taker:

    104.1. is expected to determine what constitutes a material incident by assessing the impact on its own business consistent with the guidance outlined in paragraph 62;

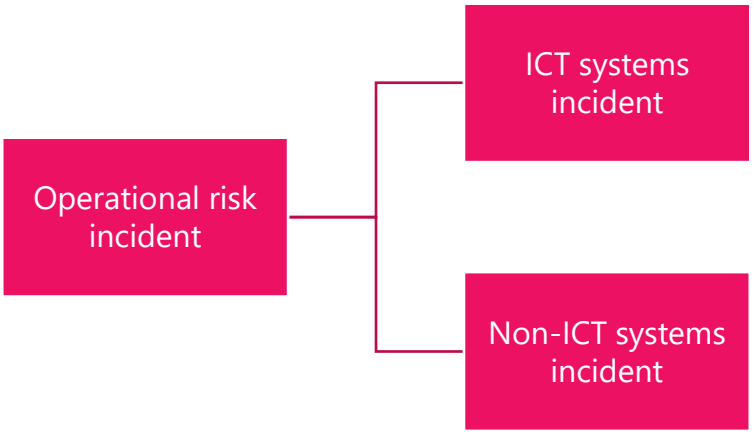
    104.2. may submit an initial report that is incomplete if certain information is not yet available within the first 72 hours and provide the missing information in subsequent reports to the Reserve Bank; and

    104.3. may amend any details previously supplied to the Reserve Bank if those details are later found to be incorrect or inaccurate.

105. The 72-hour period starts from the time the incident is determined to be material. The Reserve Bank may also request additional information from the deposit taker regarding the incident reported as a part of ongoing supervisory engagement relating to the incident.

106. For reporting purposes, an operational risk incident can be an ICT systems incident or a non-ICT systems incident (Figure 5).

Figure 5: Relationship of operational risk incident and ICT systems incident reporting requirements



107. The requirements in clause 21 are not intended to duplicate the material operational risk incident reporting requirements in clause 16. As all material ICT systems incidents are also material operational risk incidents, we expect to receive only a single report for the same incident. Where a material ICT systems incident occurs, a report submitted under this requirement will be treated as satisfying both the material ICT systems incident reporting requirement and the material operational risk incident reporting requirement. We would, however, still expect a report for any material operational risk incident that is not an ICT systems incident.

108. The intent of the reporting requirements is for the Reserve Bank to be adequately informed of a material incident affecting a deposit taker when it happens, but in a way that is efficient and not unnecessarily burdensome to the deposit taker.

109. The Reserve Bank provides reporting templates that are available on the website.[2] These templates are intended to support consistent and efficient reporting, but their use is not intended to prescribe how a deposit taker designs its internal incident identification or information collection processes.

Part 5: Management of risks related to material service providers (MSPs)

110. Part 5 sets out requirements for a deposit taker relating to the management of risks from using MSPs. These requirements support deposit takers in managing their operational risk as the provision of critical operations by third party service providers means that deposit takers have less direct control over how these risks are managed. Proactive management of these risks is important for ensuring that deposit takers can ensure their own operational continuity, both in business-as-usual times and in resolution.

111. The requirements in this Part also relate to requirements in the Outsourcing Standard. Specifically:

    111.1. The Operational Resilience Standard sets out overarching requirements for all MSP arrangements, and the purpose of these requirements is to support the business continuity and operational resilience of deposit takers.

[2] See: Cyber resilience for regulated entities - Reserve Bank of New Zealand - Te Pūtea Matua

111.2. The Outsourcing Standard sets out additional requirements necessary to ensure sufficient controls are in place for such arrangements if a resolution event arises.

112. We expect deposit takers to think about implementation of requirements in both Standards holistically.

Meaning of material service provider and arrangement (Clause 22)

113. Clause 22 sets out the definition of an MSP and arrangement. An MSP in relation to a deposit taker means a third party who provides the deposit taker with a critical operation. This will be under an MSP arrangement, which is a contractual arrangement between the person and the deposit taker for the provision of critical operations to the deposit taker on a regular or continuing basis.

113.1. A service provider may be identified as material as a result of an individual arrangement or multiple arrangements with a deposit taker.

113.2. A fourth party is a party that an MSP relies on in delivering services to a deposit taker. A deposit taker is expected to be aware of any material fourth parties that are critical for the MSP in providing its services to the deposit taker. A fourth party is also referred to as an 'indirect arrangement' in Schedule 1 of the Standard.

Scope of, and requirements for, arrangements with material service providers (Clause 23)

114. Clause 23 requires a deposit taker to ensure the critical operations undertaken by an MSP meet the tolerance levels that they set for those critical operations. Clause 23(2) requires that before entering into an arrangement with an MSP, a deposit taker must conduct an adequate inquiry into the ability of the MSP to meet the requirements of the deposit taker. Clause 23(3) sets out what a deposit taker is required to do for each arrangement with an MSP.

115. We expect adequate inquiry under clause 23(2) could include, but not be limited to:

115.1. a competitive selection process; and

115.2. an assessment of the financial and non-financial risks from reliance on the service provider, including risks associated, for example, with geographic location or concentration of a service provider or a party the service provider relies on in providing the service.

116. Clause 23(3)(a) requires a deposit taker to document and monitor the terms of the agreement. As a matter of good practice, the agreement could include:

116.1. the specification of the services covered by the agreement and associated service levels;

116.2. the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity;

116.3. provisions to ensure the ability of the entity to meet its legal and compliance obligations;

116.4. provisions for notification by the service provider of its use of other MSPs that it materially relies upon in providing the service to the deposit taker through sub-contracting or other arrangements;

116.5. provisions for the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;

116.6. a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event;

116.7. have termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement; and

116.8. provisions which allow the Reserve Bank to;

116.8.1. access to documentation, data and any other information related to the provision of the service;

116.8.2. conduct an on-site visit to the service provider; and

116.8.3. ensure the service provider agrees not to impede the Reserve Bank in fulfilling its duties as prudential regulator.

117. To comply with clause 23(3)(a)(ii), we expect deposit takers to test the BCP capability to ensure it is appropriate and adequate. This testing is expected to be adequate to provide assurance that the deposit taker continues to be able to provide the critical operation(s).

Policies for service provider management (Clause 24)

118. Clause 24 requires a deposit taker to establish and maintain a documented policy for the management of its MSPs and identify, manage and mitigate the operational risks associated with MSPs. This is known as a material service provider management policy.

119. The maintenance of a board-approved material service provider management policy best supports the ultimate outcome of a deposit taker having appropriate measures in place to oversee and manage the risks arising from the use of MSPs.

120. Clause 24(2) sets out what a deposit taker is required to document in its policy. As a matter of good practice, a deposit taker is encouraged to include the following aspects within its policy:

120.1. underlying methodology for the assessment of the MSPs;

120.2. MSP on-boarding and exiting procedures;

120.3. BCPs and alternative arrangement considerations (including where the service provider is unable to provide the service for an extended period of time);

120.4. issues management and escalation procedures; and

120.5. processes for vetting key personnel of service providers.

ICT systems risks relating to use of material service providers (Clause 25)

121. Clause 25 requires a deposit taker to identify, document and undertake a risk assessment of risks posed by MSPs collected, storing and processed data for ICT-related critical operations. The intent is for the deposit taker to understand data location, access rights, data flows, and support effective oversight and incident response.

122. We expect a deposit taker to document the shared responsibilities with the MSP. This may include responsibilities for configuration, identity and access management, encryption, logging, monitoring, vulnerability management, backup, recover, incident notification and change management.

123. We expect a deposit taker to conduct an assessment on an MSP prior to its on-boarding or engagement and throughout the service engagement to ensure achievement of business performance and recovery objectives remain unimpaired, considering the latest risk environment.

124. We expect assessments to consider risks to confidentiality, integrity, and availability, including factors such as security governance, secure development lifecycle, personnel security, data location, access controls, transmission methods, and reliance on subcontractors, to inform appropriate risk mitigations.

125. Where an MSP uses artificial intelligence to provide the service, we expect the deposit taker to consider risks to data governance and assess reliability of service output generated from the MSP. We expect a deposit taker to consider supply chain risks such as vetting of personnel or subcontractors, concentration and geopolitical risk.

126. We expect a deposit taker to consider the scope, depth and independence of that assessment and take steps to address any limitations identified when a deposit taker relies on an external assessment, certification, attestation or assurance report.

127. For further information and details regarding ICT systems risks relating to use of MSPs, refer to Part D of our *Guidance on Cyber Resilience*.

Reporting requirements (Clause 26)

128. Clause 26 sets out the reporting requirements for a deposit taker relating to arrangements with an MSP. Clause 26(1)(a) requires a deposit taker to notify the Reserve Bank of the existence of an arrangement with an MSP via the critical operations and material service provider register (as per clause 26(2)). This register as aforementioned will contain information set out in Schedule 1 of the Standard.

129. Clause 26(1)(b) requires a deposit taker to notify the Reserve Bank of any material changes to existing MSP arrangements, and the notification is to be provided as soon as practicable. Examples of material changes could include, but are not limited to;

    129.1. the name of the accountable person at the deposit taker responsible for overseeing the MSP arrangement;

    129.2. changes with indirect arrangements and different fourth parties being involved, which impact in some way the ability of the third party to provide the critical operation;

129.3. a change in the substitutability of a material MSP arrangement, where a replacement provider cannot be sourced ahead of the current arrangement expiry date;

129.4. the location of data related to critical operations, with the relocation involving a jurisdiction of considered high physical or technological risk;

129.5. the service(s), function and/or critical operation being provided by the existing MSP; and

129.6. establishing a new arrangement with a current, or new, MSP.

130. Clause 26(3) requires a deposit taker to notify their board, or a designated board committee, as applicable, about how the arrangements a deposit taker has with MSPs comply with the deposit taker's policy for management of its material service providers under clause 24.

131. A deposit taker is expected to ensure that the frequency of reporting to its board supports the policy outcome of effectively managing the risks arising from the use of MSPs. A deposit taker is expected to monitor and ensure that senior management receive reporting on material arrangements commensurate with the nature and usage of the service. This monitoring is expected to include a regular assessment of:

131.1. performance under the service agreement with reference to agreed service levels;

131.2. the effectiveness of controls to manage the risks associated with the use of the service provider; and

131.3. compliance of both parties with the service provider agreement.

Part 6: Business continuity planning (BCP)

132. Part 6 sets out requirements for BCP to ensure the continued operation of critical operations for a deposit taker. Sound governance oversight is necessary for setting the parameters in which a deposit taker manages its BCP.

Business continuity plans (Clause 27)

133. Clause 27 requires a deposit taker to have an appropriate BCP for its critical operations. This enables a deposit taker to maintain those operations through defined tolerance levels should an operational disruption event occur and mitigate the impact of the disruption on its business operations.

134. We expect a deposit taker's BCP to cater to all stages of disruption to critical operations, which includes triggers and identification, initial actions (such as alternative arrangements), further actions, assessment and communications.

135. The use of contingency arrangements (where viable options exist) enables a deposit taker to respond quickly to a disruption when recovery plans do not operate as intended, including those of service providers and related parties.

136. A deposit taker may maintain one or more BCPs. It is useful to clearly link the BCP and any other management plans that deal with incidents, including disaster recovery, liquidity management and information security incident management. Alignment with crisis management governance, triggers, actions and communication plans is important.

137. Capabilities required to execute the BCP may be maintained within the deposit taker or via an arrangement with another party. Such arrangements with other parties must meet the requirements for management of service providers arrangements in clause 23 of this Standard.

Contents of business continuity plan (Clause 28)

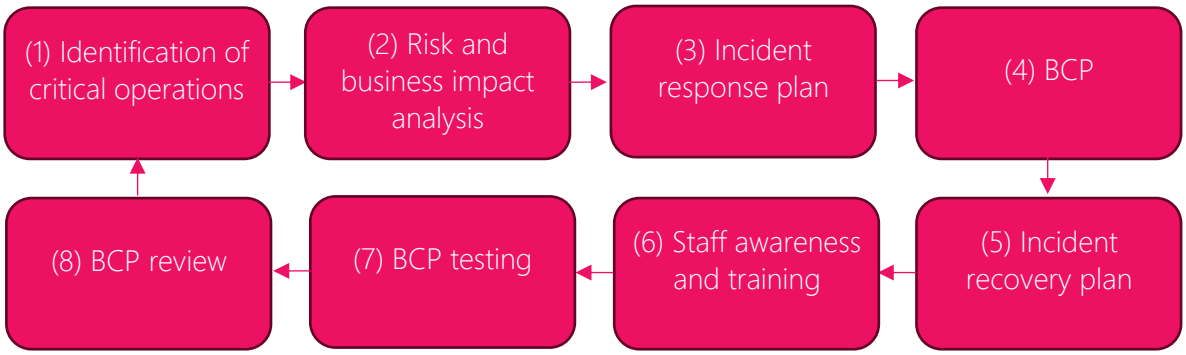
138. Clause 28 sets out how a deposit taker is to identify, manage, and respond to an operational disruption event in its BCP. Clause 28(3) highlights the requirements that do not apply to Group 3 deposit takers and overseas licensed deposit takers, which are as follows:

    138.1. 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; and

    138.2. the documentation of a communications strategy to support the execution of the plan.

139. A deposit taker's board-approved BCP is expected to be clear, as well as consistent and complementary with its incident response and incident recovery policies, where applicable. Deposit takers are encouraged to consider the generalised business continuity framework phases as illustrated by Figure 6 below.

Figure 6: Generalised business continuity framework phases



Regular testing programme (Clause 29)

140. Clause 29 requires a deposit taker to have a regular programme for testing its BCP. A deposit taker's testing programme must:

    140.1. cover every critical operation listed in the register; and

    140.2. focus on the material risks facing the deposit taker; and

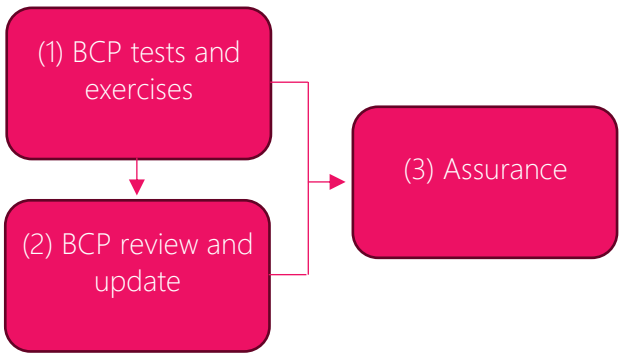
    140.3. test the effectiveness of the plan in a range of severe but plausible scenarios.

141. Clause 29(2) requires a deposit taker to conduct a test of its BCP at least once in a 12-month period. Clause 29(3) requires Group 3 deposit takers and overseas licensed deposit takers to conduct BCP testing at least once in a 24-month period.

142. Effective business continuity planning is an ongoing process - tools put in place are expected to be tested, maintained and improved to ensure that they are fit for purpose. Figure 7 (and

the accompanying text below) outlines how a deposit taker could develop its testing and assurance processes to maximise the use of the information gathered to strengthen its BCP.

Figure 7: BCP: Test, review, and assurance processes



BCP tests and exercises

143. This stage examines the fitness-for-purpose and adequacy of the BCPs. This can include assessment of staff preparedness and process soundness. The tests and exercises can be discussion based, scenario simulations (for example, performing duties in a simulated functional environment) or a combination of these two at different scales.

144. The key objective is to verify the quality, performance or reliability of system resilience in an operational environment. This phase could use quantifiable metrics to assess the operability of a system or system component, including back-ups (for example, what happens when a system or system component loses power).

145. The tests and exercises can cover the people, processes and specific aspects of a system. The comprehensiveness of the BCP tests and exercises are expected to be commensurate to the systemic importance of the deposit taker.

BCP review and update

146. Tests and exercises are expected to inform the BCP review and feed into the BCP update. The review is expected to account for the effectiveness of the deposit taker's BCPs in a range of severe but plausible scenarios, as well as consider the deposit taker's legal or organisational structure, business mix, strategy and/or risk profile.

Assurance

147. A deposit taker's internal audit function, or another independent person, is expected to assess the sufficiency and soundness of the BCP and the updates, considering the results of the tests and exercises. The deposit taker is expected to be able to reassure its board that the BCPs are sufficient and feasible to maintain its critical operations within tolerance levels through disruptions, and it will be required to assure the board that testing procedures have been conducted and are adequate (as highlighted in clause 30).

Reviews of business continuity plans (Clause 30)

148. Clause 30 requires a deposit taker to review its BCP on a regular basis and reflect any changes to its legal or organisational structure, business functions or business lines, or operational risk profile.

149. We note there is a distinction between business functions and business lines. Business functions are internal departments and capabilities (for example, Finance, Marketing) focused on specific tasks to keep the firm running. Business lines (or lines of business) are distinct business units focused on selling specific products/services to specific customer segments. Therefore, the business functions focus on "how" work gets done, whereas the business lines focus on "what" is sold.

150. We expect BCP reviews to be conducted at least once every 3 years, with more regular periodic reviews conducted as required commensurate with a deposit taker's size and nature of business.

151. We expect BCPs to be informed by results of testing, review findings, internal audit findings and lessons learned from actual business disruptions. Furthermore, any review and associated updates is expected to be carried out as soon as possible after a material change in a deposit taker's structure, business or risk profile – for example, after a merger or acquisition or a material external shock.

Assurances relating to business continuity plans (Clause 31)

152. Clause 31 requires a deposit taker to, provide, on a regular basis, its board with an assurance that the deposit taker's BCP for critical operations:

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

    152.2. has been adequately tested.

153. Internal audit, or another operationally independent person, provides an important vehicle for assurance for a deposit taker. The board may consider seeking assurance through expert opinion or other means to complement internal audit. An audit program would typically assess all aspects of business continuity capability over time. Additional assurance projects could be triggered by changes to services, processes, information assets, the business environment and stakeholder expectations.

Activation of business continuity plans (Clause 32)

154. Clause 32 requires a deposit taker to notify the Bank, in the event of a deposit taker activating its BCP for critical operations, as soon as possible and, in any case, no later than 72 hours after the activation. We expect earlier notification and engagement to support supervisory engagement.

155. This notification may be included in the deposit taker's material operational risk incident or material ICT systems incident reporting (in which case no separate reporting is required under this clause but we expect that the BCP response would be included as part of the relevant reporting). Clauses 16 and 21, and the accompanying guidance above, provide further detail on material operational risk incident and material ICT systems incident reporting.

Part 7: Governance responsibilities

156. Part 7 sets out governance responsibilities, including for a deposit taker with subsidiaries (that is, head of a group), and our expectations around ensuring that the requirements of this Standard are met by the board and senior management of a deposit taker.

Responsibilities of board (Clause 33)

157. Clause 33 sets out the responsibilities of the board of a deposit taker under the Standard. We do not, however, expect the board to be involved in the day-to-day monitoring and managing of all operational risks. Rather, the board's responsibilities are focused on approving and overseeing the underlying policies and processes, as set out in clause 32 of the Standard.

158. Requirements for board responsibilities apply equally across all deposit taker groups given their fundamental importance. For further information and details regarding board responsibilities, refer to Part 2 of the Governance Standard.

Responsibilities of senior management (Clause 34)

159. Clause 34 sets out the responsibility of senior management to manage the operation of a deposit taker's operational risk management framework. This includes:

    159.1. monitoring and managing all operational risks to the deposit taker consistent with the policies and processes approved by the board; and

    159.2. developing the operational risk management policies and processes in the organisation for approval by the board.

160. We expect senior managers to actively manage risks within their respective areas, clearly define and communicate risk responsibilities and collaborate effectively to address cross-cutting risks while promoting a strong risk culture (refer to Part 5 of the Risk Management Standard and accompanying Guidance document for further details around risk culture). We expect accountability mechanisms to be in place to ensure that boards and senior managers take appropriate (sustainable) and timely actions (via risk mitigation and/or risk acceptance) and that risk remediation, monitoring, notification, and reporting are implemented in response to all material risks.

Group requirements (Clause 35)

161. Clause 35 sets out requirements for a deposit taker that operates as the head of a group. In this context, the group comprises the deposit taker and its subsidiaries, or other entities covered by the deposit taker's conditions of licence. Where a deposit taker operates as group head, it is responsible for the operational resilience of the group as a whole, including the management of material operational risks arising across group entities, whether located in New Zealand or overseas. This includes:

    161.1. maintaining a group-level operational risk management framework that addresses material operational risks across the group, including risks relating to ICT systems and MSPs, noting that clause 12 and the corresponding guidance set out expectations relevant to application at a group level;

    161.2. ensuring that critical operations conducted by entities within the group are supported by effective business continuity arrangements aligned with group-approved tolerance levels and capable of being executed when required, noting that clauses 27 and 28 of the Standard and the corresponding guidance provide further detail relevant to group arrangements; and

161.3. ensuring that the Reserve Bank is notified of an operational risk incident (whether an ICT systems incident or non-ICT systems incident) affecting the group where the incident is likely to have a material impact on the group's financial position or its ability to maintain critical operations, noting that clauses 16 and 21 of the Standard and the corresponding guidance set out expectations for incident notification.