Reserve Bank of New Zealand
Te Pūtea Matua

Risk Management Standard

Guidance Note

GN XX.1

Guidance Note version history

February 2026	Consultation draft for exposure draft of the Risk Management Standard	Relates to Risk Management Standard exposure draft version dated [February 2026]
Day Month 20XX	First issue date	Relates to Risk Management 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 paper 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

Guidance Note version history 2
Use and status of this Guidance 5
Part A. Introduction to the Risk Management Standard 6
Overview 6
Proportionality 6
Context and background 7
Part B. Detailed guidance on the Standard 9
Subpart 1: General provisions (Clauses 3-6) 9
Subpart 2: Risk management frameworks (Clauses 7-15) 9
Risk management frameworks (the Framework) (Clause 7) 10
Consideration of risks (Clause 8) 13
Framework features (Clause 9) 14
Other requirements for frameworks (Clause 10) 15
Group requirements for frameworks (Clause 11) 15
Risk appetite statement (the Statement) (Clause 13) 18
Documentation requirements (Clause 14) 20
Notification requirements (Clause 15) 20
Subpart 3 Operational requirements (Clauses 16-28) 21
Setting risk management policies and processes (Clause 16) 21
Monitoring and notification procedures (Clause 17) 21
Use of models (Clause 18) 21
Problem assets (Clause 19) 21
Contingency arrangements for stress conditions (Clause 20) 22
Management of conflicts of interest (Clause 21) 22
Reviews (Clause 22) 23
Implementation of review recommendations 24
Conduct of reviews (Clause 23) 24
What a comprehensive review covers 25
Regular stress-testing programmes (Clause 25) 25
Adequate management of information and data (Clauses 27 and 28) 27
Subpart 4 Internal controls and functions (Clauses 29-34) 29
Internal control structures (Clause 29) 29
Requirement for risk management function (Clause 30) 29
Chief Risk Officer (CRO) (Clause 31) 30
Requirement for compliance and internal audit functions (Clauses 32-34) 30
Internal audit function 31
Subpart 5 Organisational responsibilities and practices (Clauses 35-37) 32
Responsibilities of boards and senior management (Clauses 35-36) 32

Risk culture (Clause 37) 32

Use and status of this Guidance

The purpose of this Guidance is to assist licensed deposit takers (or deposit takers) to interpret and comply with the Risk Management Standard (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 is provided to assist individual deposit takers with their own compliance and a more consistent approach across the industry.

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 have been made aware of differing interpretations by deposit takers.
- Providing examples of matters deposit takers are expected or encouraged to consider when complying with requirements in 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.
- The Guidance does not necessarily cover every clause in the Standard. Given its status as an interpretation aid, where we feel a clause (when read in conjunction with the explanatory note attached to the Standard) is sufficiently self-explanatory, no additional Guidance is being provided.
- In 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.
- We will periodically 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 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 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 26 February 2026.
- We welcome feedback on the Guidance at any time.

Part A. Introduction to the Risk Management Standard

Overview

1. The purpose of this document is to provide guidance in complying with the Standard and encourage better risk management practice.

2. The guidance set out in this document discusses some good practices in meeting requirements for deposit takers. It is not intended to be exhaustive.

3. The Standard sets out requirements for deposit takers and overseas licensed deposit takers (branches) in relation to:

    3.1. developing a risk management framework (Framework), including a risk management strategy (Strategy), risk appetite statement (Statement) and associated policies and processes;

    3.2. developing internal processes and information systems to monitor risk and undertaking forward looking stress-testing covering all material risks; and

    3.3. adequately resourcing and providing authority and sufficient independence to risk management, audit and compliance functions.

4. Effective risk management contributes to both the soundness of individual deposit takers and the stability of the financial system as a whole. An organisation's internal controls are an important component of an entity's risk management practices.

Proportionality

5. Our expectations for deposit takers vary depending on the size, nature and complexity of operations of individual deposit takers. A deposit taker's Framework must be commensurate with the size and nature of their business and complexity of its operations. This helps to ensure that the required content of a Framework is proportionate and tailored to the different circumstances of individual deposit takers. We provide some key points below regarding each of these three areas of consideration:

    5.1. size: business size refers to the size of the deposit taker's operations, including the size of the deposit taker's balance sheet regarding the amount of held assets. Other aspects of size could include the number of employees and the number of locations of the deposit taker. The Proportionality Framework sets out thresholds relating to the total asset size of each group.

    5.2. nature: the nature of a deposit taker's business refers to its core activities and functions. This encompasses what a deposit taker does as well as how it operates and ultimately its connectedness to the economy and the other entities in the financial system. For example, the deposit taker's role in managing money and assets and the services provided to individuals and other businesses.

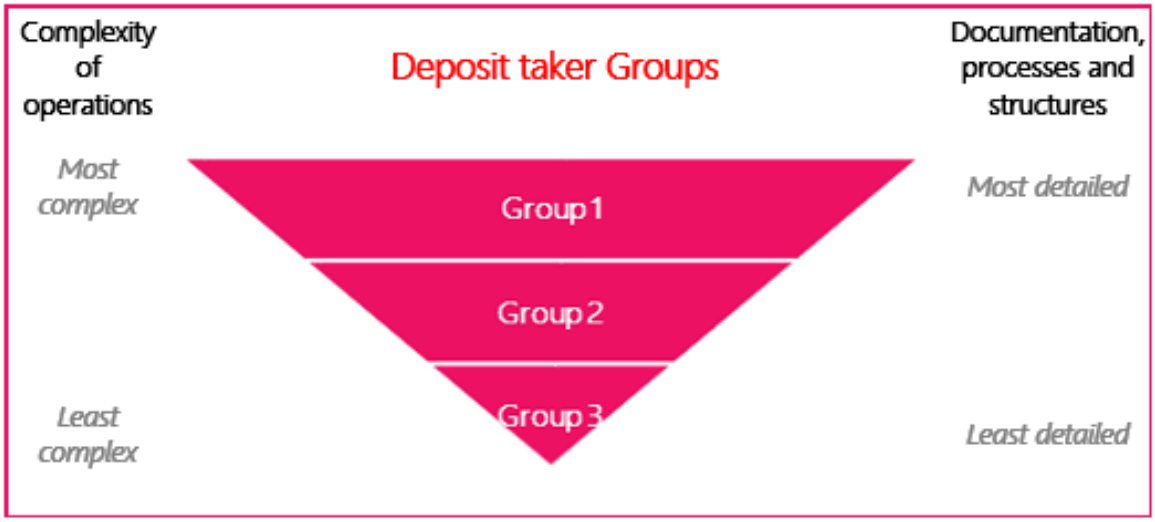
    5.3. complexity: a deposit taker's complexity refers to the relative complexity of its operations. It includes the formation of interconnected technologies across operations, data held/used in the deposit taker, the range of offered products and services, the number of people (for example employees, customers, borrowers, depositors), and the complexity of organisational legal structure more broadly.

6. Note that these 3 concepts are not mutually exclusive and tend to be correlated. However, there are examples of large deposit takers that offer products that are not complex (for example residential mortgages) and other entities that are small and bespoke but offer very complex and diverse products.

7. The requirements in the Standard are designed to be sufficiently flexible so that deposit takers can tailor their risk management practices to their individual circumstances and still comply with the requirements. This guidance provides examples of how our expectations might vary depending on the size, nature and complexity of operations of a deposit taker for each component of the Standard. Not all of the practices outlined in this guidance are relevant for every deposit taker and some aspects may vary, as noted above, depending upon the size, nature and complexity of operations.

8. The documentation, for example, of larger deposit takers and/or those with more complex operations would typically be expected to have greater specificity than the documentation of relatively smaller deposit takers with less complex operations (Figure 1). Similarly, we would expect the processes and organisational structures of the larger deposit takers with more complex operations to be more detailed compared to smaller deposit takers with relatively less complex operations.

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



Context and background

9. The information in this guidance supports meeting the requirements of the Standard. It is intended to be read alongside the Standard. In some cases, the Standard is supplemented by requirements in other standards that are specific to individual risk categories. For example, the Liquidity Standard requires deposit takers to have a contingent funding plan, which may form part of their framework. Where relevant, the guidance signposts deposit takers to these relationships between standards.

10. Our intended policy outcomes for the Standard are set out below in Table 1.

Table 1: Key policy outcomes in developing the Standard

Key policy outcomes
1. To incentivise deposit takers to have dynamic and evolving risk management practices commensurate with their risk profile and systemic importance, and which are responsive to a changing risk environment.
2. To best position deposit takers for managing cross-cutting risks (such as climate-related), event risks (such as cyber or conduct) and secular risks (such as complacency or risk appetite creep), as well as to understand how various risks relate to, and interact with, each other (such as for example how climate risk impacts credit risk through a potential increase in defaults on loans by business and households affected by adverse climate events).
3. To ensure deposit takers have appropriate risk data to support decision-making and reporting requirements in both normal operating conditions and stress conditions.
4. To support deposit takers to use findings from risk assessments to minimise the likelihood and impact of risks and to be better prepared for proactively responding to risk.
5. To support meaningful supervisory engagements on risk management and enable better risk management practices across deposit takers.

Part B. Detailed guidance on the Standard

Subpart 1: General provisions (Clauses 3-6)

11. The purpose of the Standard, as noted in clause 3, is to promote effective risk management practices for deposit takers and to ultimately minimise the likelihood of risks affecting the stability of the financial system.

12. To meet the requirements of the Standard, as noted in clause 6, deposit takers must:

    12.1. 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; and

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

Subpart 2: Risk management frameworks (Clauses 7-15)

13. A comprehensive Framework would be both adequate to achieve the objectives of the Standard, and be commensurate with the size and nature of its business. The Standard requires that Frameworks must, at a minimum, include:

    13.1. the board-approved Strategy (see the below section *Risk management strategy* (the Strategy) *(Clause 12)* for further details);

    13.2. the board-approved Statement (see the below section *Risk appetite statement* (the Statement) *(Clause 13)* for further details);

    13.3. clearly defined and documented roles, responsibilities and reporting structures;

    13.4. procedures for monitoring and reporting risk exposures, risk issues and breach or non-compliance issues;

    13.5. policies and processes related to the validation, approval and use of any models to measure components of risk;

    13.6. policies and processes related to the early identification and management of problem assets, including the classification and valuation of these assets;

    13.7. policies and processes related to establishing and maintaining appropriate contingency arrangements to address risks that may materialise and actions to be taken in stress conditions;

    13.8. policies and processes related to identifying, monitoring and managing potential and actual conflicts of interest;

    13.9. procedures for review of the Framework and risk management function;

    13.10. appropriate internal processes for assessing their overall capital adequacy and liquidity risk management;

    13.11. forward-looking stress testing, including how the results of stress testing programmes are integrated into decision-making, risk management processes and the assessment of their capital and liquidity levels;

13.12. information management systems and risk data aggregation and reporting capabilities; and

13.13. risk management (including the Chief Risk Officer (CRO)), compliance and internal audit functions; and internal control Frameworks.

Risk management frameworks (the Framework) (Clause 7)

14. The overarching requirement in the Standard, as set out in Clause 7 of the Standard, is that all deposit takers must have a risk management framework. A Framework can be understood as 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 risk.

15. We encourage deposit takers to use the Three Lines Model as part of having a Framework. The Three Lines Model is a widely adopted structure for clarifying roles and responsibilities for managing risks across an entity. The structure helps enhance accountability and strengthen independent oversight of a deposit taker's risk management activities. Regular communication and coordination across the 3 lines, supported by strong senior management and board oversight are essential to effectively embedding the structure.

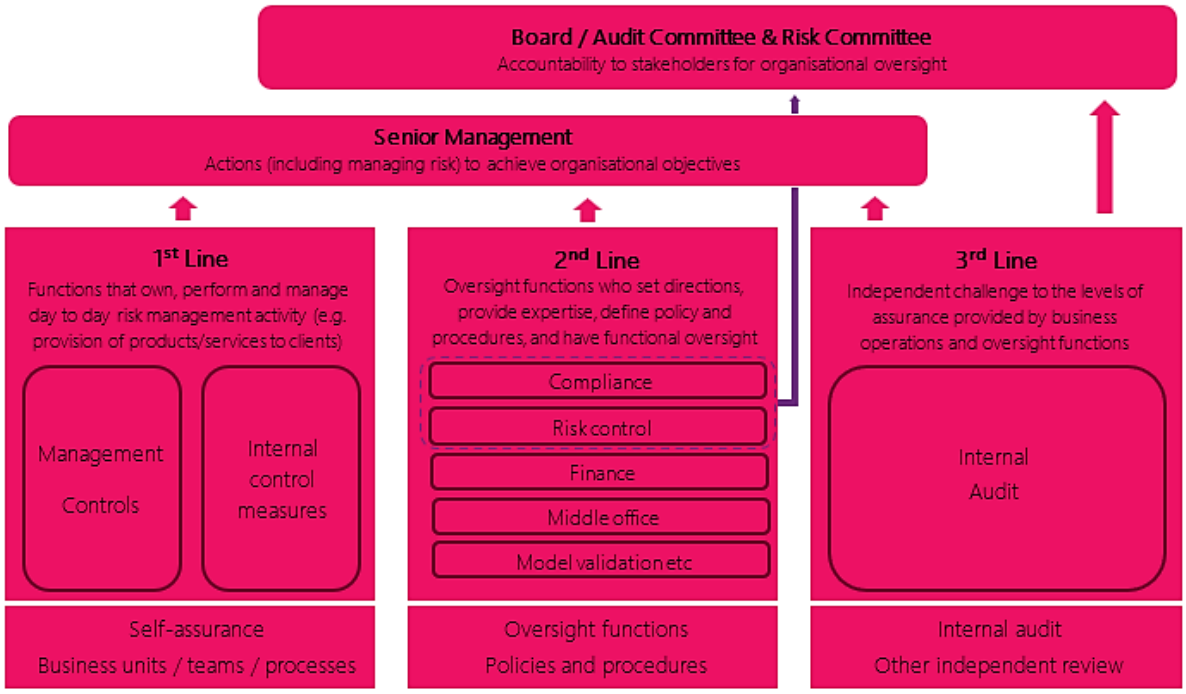
16. Its implementation is largely dependent on the deposit taker's size and operational complexity. While the specific application of this model may vary between deposit takers, the first part of Table 2 provides an example. This guidance refers to the Three Lines Model described in Table 2 below, but individual deposit takers would be expected to consider how best to give effect to this, while considering the size, nature and complexity of their business and associated operations.

Table 2: Three Lines Model – Functions

Line	Function
First line	The first line (business/operational management) consists of front line business units which own the risks and carry out the day-to-day risk management within their areas of accountability and implement the Framework (e.g. retail banking, lending teams, information technology, operations). The first line has responsibility over the internal controls, which serve as checks and balances. With the first line embedding risk management into day-to-day activities and decisions, it forms the foundation of a strong risk culture. Their core responsibility is owning and managing the risks associated with their business activity - Identifying, assessing and mitigating risks; implementing effective controls; and ensuring compliance with risk policies and procedures. For example, a lending officer performing credit checks and applying credit policy, or branch staff carrying out anti money laundering checks.
Second line	The second line (risk and compliance oversight) is responsible for setting the Framework and policies, providing review and challenging the first line. The second line oversees and challenges risk-taking activities to ensure material risks are identified, monitored and managed effectively. It evaluates the robustness of controls and mitigation strategies implemented by the first line and strengthens governance through risk reporting. The

Line	Function
	second line also plays a critical role in promoting risk awareness across the entity by providing guidance and advice. The second line needs to be independent of the business in the first line. The second line provides core risk management knowledge and skills and they hold the first line business to account. It often comprises multiple functions and multiple teams, for example the risk management function, compliance function, and risk specialist teams. Typically, a compliance function assists senior management in effectively managing compliance risks and it is complementary to the risk management function (both compliance and risk management functions are second line functions) described in clause 32 of the Standard and discussed below in *Requirement for risk management function (clause 30)*. Similarly, an ICT (Information and Communications Technology) security function focuses on managing all ICT-related and cyber security risks. This ultimately supports sound and prudent risk management in the deposit taker.
Third line	The third line is the independent internal audit function that is described in clause 32 of the Standard. The third line provides independent audit and assurance on the effectiveness of the Framework, internal controls and governance processes. It identifies weaknesses and areas for improvement, supporting proactive risk management and compliance with internal policies and regulatory requirements. The third line is responsible for providing the board and senior management with assurance that the business is managing risk appropriately. In doing so, the function helps reduce the risk of loss or damage to a deposit taker. For example, this may include the third line independently assessing and reporting on the work of both first and second lines.

Figure 2: Three Lines Model – Visualisation



17. An effective Three Lines Model has clearly assigned control and risk management responsibilities both within, and between, respective business functions which ultimately enable successful coordination and execution of control responsibilities between the 3 lines. It is important that each individual line understands and knows its assigned scope of responsibilities and how these relate to the activities of other lines.

18. Outside of any operative Three Lines Model, any external sources of assurance (including auditing) could come from an external auditor. External auditors sit outside the formalised three lines, and can provide deposit takers with independent assessment, assurance or audits of the deposit taker's three lines. While external auditors provide an additional external source of assurance on a deposit taker's risk management arrangements, we expect the internal audit function to primarily provide independent assurance for the deposit taker.

19. Regulators also sit outside of any operative Three Lines Model and are not responsible for the risk management of a deposit taker. Our role is to protect and promote the stability of New Zealand's financial system. In doing so we monitor deposit takers against their prudential requirements and take action as appropriate. We take a risk-based approach to supervision. Further information on how we see our role can be found in the Statement of Prudential Policy.

20. Deposit takers can take various actions to support the implementation of the Three Lines Model and clarify roles and responsibilities and strengthen independence across lines. The list below highlights some examples of good practice relevant for most deposit takers, although we acknowledge that smaller deposit takers may not have the resourcing to undertake each practice:

    20.1. reviewing roles and responsibilities of the first and second lines to ensure appropriate separation,

    20.2. providing training, workshops, and clear guidance to enhance understanding and awareness,

    20.3. ensuring there is regular engagement between the three lines to prevent overlaps, including developing integrated audit plans to coordinate auditing activity and avoid duplication,

    20.4. ensuring there are sufficient and adequately experienced staff across all three lines,

    20.5. appointing 'risk champions' within business units to advocate and promote sound risk management practices and provide support, training and guidance to staff on risk related matters and compliance with risk standards,

    20.6. conducting independent reviews of the three lines model and the effectiveness of the risk management and internal audit functions to ensure they are fully embedded and operating effectively, and

    20.7. engaging external consultants and group internal audit where necessary to review and provide input on internal audit plans, ensuring adequate coverage of material and emerging risks.

21. In contrast, poor risk management practices could ultimately lead to an ineffective duplication of effort, lack of accountability, and an undermining of overall risk culture in the deposit taker. It is therefore important for a deposit taker to establish clearly which

functions are responsible for identifying, assessing and mitigating certain risks so that responsibilities are not inadvertently shared or overlooked.

Consideration of risks (Clause 8)

22. The Standard requires deposit takers to assess whether an event, circumstance or trend could give rise to a risk and then assess whether that risk is material for its business.

23. The Standard sets out that effective Frameworks should focus on any event, circumstance, or trend that has the potential to give rise to a risk to its business, and have a process for identifying and managing a broad spectrum of risks (current and evolving) across the entity to ensure comprehensive ongoing oversight.

Material risks

24. Clause 7(1) requires a deposit taker to have a framework that takes in consideration all material risks. Clause 7(3) defines a material risk to be a risk that is more than minor and could have an impact on the safety and soundness of a deposit takers business or its ability to comply with its prudential obligations (as defined in the DTA, and including an obligation from any standard, regulation, or condition of licence made under the DTA, or obligation imposed by the DTA itself). Clause 8 of the Standard requires deposit takers to assess risks and determine their materiality.

25. The list below provides examples of types of risk that could be material, noting that the deposit taker itself has responsibility to assessing what risks are material to its business. The criteria or factors used for determining material risks would be clearly documented in the Strategy (including quantitative and qualitative factors such as impact on business objectives, protection of customer interest, entity reputation and financial and operational stability). We note that certain processes or events can heighten or amplify risks and increase their materiality for example, a business change process can affect a range of risks.

26. All deposit takers will individually face different sources and types of risk, and these could for example span (but are not limited to) the following risk categories:

    26.1. operational risk (including cybersecurity risk),

    26.2. compliance risk,

    26.3. credit risk,

    26.4. governance risk,

    26.5. liquidity risk,

    26.6. interest rate risk,

    26.7. concentration risk,

    26.8. market risk,

    26.9. model risk,

    26.10. outsourcing risk,

    26.11. reputational risk,

    26.12. resolution risk,

26.13. strategy risk, and

26.14. systemic risk.

27. The Standard identifies categories of risk that the Framework must, at a minimum, cover. These risk categories are interrelated and overlapping, and therefore we expect deposit takers to consider risk holistically.

28. We expect deposit takers to take ownership of their Framework, and identify the most material risks and make them priorities for controls, policies, and procedures to address these risks. This can be achieved, in part, through a Strategy that communicates the deposit taker's approach to risk management, as well as through a clearly articulated Statement that outlines the deposit takers risk appetite and risk tolerances within its risk capacity.

29. The Standard includes requirements that are relevant to the effective management of all risk categories. This is supported by risk management requirements in other standards that are only relevant for specific risk categories. For example, the Liquidity Standard includes a requirement for deposit takers to have a contingent funding plan. We expect that this contingent funding plan would form part of a deposit taker's Framework.

30. Communicating what the deposit taker views as material is important to ensure that its approach is understood by its staff and is consistently applied across its operations. We expect a well-defined risk taxonomy to be embedded in the Framework and related risk policies. This enables consistent terminology and uniform understanding, interpretation and classification of risks across the entity. A risk assessment matrix should also be used to identify and monitor emerging risks and develop forward-looking metrics, assessing risks and determining mitigating strategies and controls.

Examples

31. A Group 3 deposit taker might have a relatively less complex modelling function than a Group 1 deposit taker, given the nature of its business. The Group 3 deposit taker might therefore be expected to place less focus in relative terms on managing model risk than a Group 1 deposit taker. However, we would still expect a Group 3 deposit taker to be able to demonstrate that they had considered sources of model risk in developing and reviewing their Framework.

32. We expect the deposit taker to give careful consideration to the interconnectedness of material risks. It is important for a deposit taker to assess situations where the probabilities of two material risks occurring, or two mitigating actions not succeeding, are correlated (for example, an earthquake damages physical and technological infrastructure which leaves individuals temporarily unable to make mortgage payments as a result of the natural disaster incident).

33. This is also an important consideration for the scenario design stage of stress testing (clauses 25 and 26).

Framework features (Clause 9)

34. Clause 9 sets out key feature requirements of a Framework. Clause 9 of the Standard requires a deposit taker's Framework to be strategic and forward-looking, and consider risks across different time horizons and from internal and external sources. This requirement relates to how decision-makers assess and create future opportunities and

predict business conditions, and includes forward-looking factors, such as changes in the deposit taker's business strategy and risk profile, and risks arising from the macroeconomic environment.

35. We expect that decision-makers are considering risk across the near- and longer-term and consider forward-looking factors such as changes in the deposit taker's business strategy and risk profile. This includes present and future threats, risks and opportunities. The risk owner, metrics, board approved limits and governance committee for each material risk should be clearly outlined in the Framework to ensure transparency and accountability.

Other requirements for frameworks (Clause 10)

36. Clause 10 of the Standard sets out other requirements for the Framework, in addition to clauses 7-9. These are elaborated on in clauses 12, 13, 22, 25, 27, 29, 30 and 32-34 (discussed below).

Group requirements for frameworks (Clause 11)

37. Where a deposit taker is part of a group, it is required to consider risks from related parties within the group in its Framework and apply requirements of the Standard on a group-wide basis (e.g., from its parent, any subsidiaries or related companies it may have, or any branches operated by group members). We expect risk to be managed through a whole-of-group approach (noting that overseas regulators would impose requirements at the global group level) and must be managed at a New Zealand group level and at the individual deposit taker level.

38. As highlighted in clause 11(2) of the Standard, regarding group requirements deposit takers must apply the requirements of this standard on a group-wide basis. Where a deposit taker is part of an overseas deposit taker (i.e., it is an overseas licensed deposit taker or "branch"), the Standard allows a deposit taker to meet the requirements of the standard by using group-level Frameworks, policies and procedures as long as New Zealand-specific prudential requirements are met, and the board of that deposit taker (or New Zealand CEO in the case of a branch) is satisfied that the requirements are met in respect of that deposit taker. This would enable a deposit taker to utilise a group-level Framework, should one exist, as we consider it desirable for risk management to be consistent across the group.

39. Where a deposit taker deems it as appropriate, it may have its own Framework, for example in the case of a locally incorporated subsidiary. Reviews of wholly owned subsidiaries' Frameworks by the parent would be expected to focus on alignment and adherence to the group framework, and assess whether the subsidiary's Framework is fit for purpose in the New Zealand context. With our proposed approach, we expect group level Frameworks to be broadly appropriate for the New Zealand context given the high degree of international alignment between these requirements and international good practice. We expect key policies and procedures taken from the group Framework to be reviewed and approved through local governance to ensure they are fit for purpose before adoption.

40. We expect that the appropriateness of using a group Framework would be assessed by that deposit taker according to the size and nature of business of the deposit taker, and the complexity of its operations. The purpose of this assessment is to ensure that the group-level framework is 'fit for purpose' for the institution. We expect that the assessment would be conducted prior to using the group-level framework and after any

changes to the group or the institution that may materially impact on the Framework. It must also be appropriately documented.

41. We expect deposit takers to have a clear understanding of the reliance on, and interaction with, the group's Framework and understand the consequences of these arrangements for the risk profile of the deposit taker.

Risk management practices at different consolidation levels

42. In situations where the deposit taker is a member of a group, we expect the deposit taker to clearly demonstrate effective risk management practices at different consolidation levels (i.e. for the deposit taker, and the deposit taker and its subsidiaries).

Risk management strategy (the Strategy) (Clause 12)

43. Clause 12 of the Standard requires all deposit takers to have a board-approved Strategy. We expect an effective strategy to be:

    43.1. strategic in nature,

    43.2. digestible by the board,

    43.3. aligned with a deposit taker's business strategy, and

    43.4. approved by the full board rather than being delegated to the Risk Committee (as the Strategy needs to be considered alongside the business strategy).

44. Effective risk management strategies must:

    44.1. Describe each identified material risk and the adopted structured approach to effectively manage these risks. We expect the Strategy to include coverage of both existing and emerging risk(s);

        44.1.1. We note that identification of cross cutting risks can be challenging, particularly in larger more complex entities, where the risk of silos is higher. A structured approach using forward-looking tools such as scenario analysis, stress testing, PESTLE (political, economic, social, technological, legal, and environmental) or SWOT (strengths, weaknesses, opportunities, and threats) analysis, horizon scanning, workshops and meetings can support early identification and management of emerging and cross cutting risks. Advanced tools such as data analytics and Artificial Intelligence (AI) can further strengthen risk identification and assessment.

    44.2. Summarise the policies and processes dealing with risk management matters and describe roles and responsibilities related to the risk management function and governance arrangements; and

    44.3. Outline an entity-wide approach for ensuring awareness and understanding of the Strategy.

45. We expect that a Strategy would contain sufficient information to communicate, in general terms, the deposit taker's entity-wide approach to risk management. It is a document that describes, in summary form, each identified material risk and the deposit

taker's approach to managing material risks, while the Framework operationalises the Strategy by identifying how a deposit taker manages risk.

46. Deposit takers are best placed to determine elements of their own Strategy, and Statement, that would most effectively enable and support sound risk management practices. An effective Strategy determines how a deposit taker treats material risks, following their initial risk identification and subsequent assessment, as demonstrated below in Figure 3.

Figure 3: Risk management cycle

47. The list below provides a brief description regarding each stage of the risk management cycle.

    47.1. Identify: documenting both crystallised and emerging risk(s) that could affect the deposit taker.

    47.2. Measure: evaluating the identified risk(s) to better understand the potential magnitude and breadth of impact for the deposit taker, and the likelihood of occurrence.

    47.3. Evaluate: analysing the measured risk(s) to determine the severity and prioritisation required for managing it going forward.

    47.4. Monitor: having regular ongoing checks and processes in place for continued surveillance around the how the risk(s) is/are developing and how implemented strategies are working.

    47.5. Report: documenting and highlighting key developments regarding the efficacy of the risk management process in place for the identified risk(s).

    47.6. Control: implementing controls to manage and mitigate the identified risk(s).

48. The Strategy must be reviewed annually (see clause 22), as this ensures that it is updated to reflect any broader external changes in the business environment, industry trends and

regulatory requirements. It also ensures that there is regular engagement in place with the board on the deposit taker's risk management, business strategy and appetite for risk.

49. The Strategy must also include an approach for building awareness of the Strategy. We expect that a documented communication plan would best support ongoing entity-wide awareness and understanding (using various methods such as meetings, training, intranet, and email to communicate the Strategy).

Risk appetite statement (the Statement) (Clause 13)

50. Clause 13 of the Standard requires all deposit takers to have a board-approved Statement which would be expected to be commensurate with the size, nature and complexity of the deposit taker's operations.

51. A Statement must define the level of risk the deposit taker is willing to assume, or tolerate to achieve its strategic objectives. This includes having clearly defined and well-documented appetite, metrics, limits and tolerance levels for each material risk. This Statement specifies boundaries which enable communication of risk tolerance for particular risks and monitoring of how the deposit taker is operating against its stated appetite for a particular risk. It informs the policies and processes developed for risk-taking, measurement and monitoring.

52. The articulation of risk appetite and risk tolerances is central to the Statement:

    52.1. risk appetite expresses the aggregate level, and types, of risk that a deposit taker is willing to assume to achieve its strategic objectives and fulfil its business plan before breaching its obligations or constraints determined by regulatory capital, liquidity, or other needs. Risk appetite can be expressed in several ways to ensure that it is commonly understood and consistently applied across a deposit taker. Risk appetite is generally expressed in the form of high-level qualitative statements that clearly capture the deposit taker's attitude to, and level of, acceptance of different material risks. Where appropriate, the Statement would include quantitative measures. Furthermore, while a deposit taker may have an overall risk appetite for the entity as a whole, we expect it to assign board-approved appetites to each material risk as not all risks would be expected in practice to have the same appetite.

    52.2. risk tolerances are established for each material risk, taking into consideration the deposit taker's risk appetite. It is good practice for risk tolerances to sit above the regulatory minimums (e.g capital requirements or liquidity requirements such as the mismatch ratio or core funding ratio), as this enables deposit takers to be proactive and mitigate key risks and noncompliance before it occurs.

    52.3. Risk tolerances can be expressed in different ways, depending on the nature of the risk being managed but are usually expressed as a measurable limit or indicator to best enable a clear and transparent monitoring process that ensures the deposit taker remains within the determined risk tolerance. It may not be possible to set quantitative tolerances or limits for all risks. Where a risk exposure falls outside the risk tolerance, we expect the deposit taker has a process to escalate and develop a plan to review the risk and ensure that it is promptly brought to again be within an acceptable tolerance.

52.3.1. operational limits for individual material risks would be clearly linked to risk appetite, and non-financial risks would have clearly defined, measurable risk operational limits.

52.3.2. some risks, such as types of operational risk, can be grouped together, reflecting their complex and inter-related nature, as long as no individual risks are material in their own right. They should be monitored to assess whether they could become material, as failure to do so would reduce visibility of individual risks and lead to inconsistent grouping and limited sector compatibility.

53. Clause 22 requires an annual review of the Statement. We expect that the development and review of a deposit taker's board-approved Statement would be performed as part of the broader strategic and business planning process. The Statement would provide relevant information on the board's expectations regarding the risk appetite and would in turn be updated to reflect any changes, as a result of the strategic and business planning process.

54. Risk appetite is a key consideration in developing policies in relation to key decision-making processes. For example, when a deposit taker develops a business case or agrees to contractual and service level agreements for a material service provider, we expect that the Framework would be used to identify and assess risks, and that the risk appetite is considered in the decision making and implementation process.

55. As best practice the board would demonstrate ongoing active engagement with management regarding both developing and reviewing the Statement, as well as ownership of the Statement. This might be achieved, in part, through reporting and communication processes and structures that enable the board and/or Risk Committee to:

    55.1. identify the deposit taker's overall current risk profile and how this compares to its risk appetite and capital strength;

    55.2. be satisfied that senior management's interpretation and application of the risk appetite and tolerances is appropriate; and

    55.3. appropriately align risk appetite to the approach adopted in the Framework for assessing, monitoring and managing the different material risk.

56. Deposit takers must communicate appropriate aspects of its Statement throughout its operations to ensure that the Statement is understood and consistently implemented. An appropriate summary of the Statement would include relevant information for the intended audience.

57. Where an overseas deposit taking group operates both a subsidiary and a branch in New Zealand, the Standard requires each deposit taker to have a Statement that is tailored to its risk profile. Although risk appetite may be set by the overseas group on a divisional basis, we, nevertheless, expect the branch's Statement to appropriately address the risk profile of the New Zealand branch operation.

Examples

58. We expect each deposit taker to consider its own strategic objectives and business plans when deciding what is appropriate for its own Statement. Fundamentally, every deposit taker faces different numbers and types of material risks and this would influence different

deposit taker Statements. For example, a Group 1 deposit taker may have a comparatively greater number and complexity of material risks that it faces than a Group 3 peer. Therefore, although we largely expect most Statements to be qualitative in nature, it could be reasonably expected that the Group 1 deposit taker has relatively more quantitative measures to also capture the entity's attitude to, and level of, acceptance of different risks, where appropriate.

59. Branches may choose to leverage the overseas deposit taker's Statement, but as highlighted in clause 35 of the Standard the New Zealand CEO (who is included in the interpretation of the deposit taker's board) would be ultimately responsible for ensuring that it is appropriate for the branch and a New Zealand context. This may include supplementing the overseas deposit taker's Statement with additional measures that are specific to the branch's operations. An example of this could be a measure relating to New Zealand Dollar liquidity, which may be a material risk for the branch but not for the overseas deposit taker as a whole.

Documentation requirements (Clause 14)

60. Clause 14 of the Standard requires deposit takers to ensure appropriate documentation of their Framework. The Reserve Bank does not issue any templates for deposit takers to use in developing any components of their Framework, including the Strategy and Statement. The documentation of a Framework and its components is left to the discretion of the individual deposit taker.

61. Deposit takers can, as good practice, document their Framework as a combination of multiple documents, which would be easily digestible for wider internal dissemination (e.g. to the board), with an overarching summary document that at a high level sets out and explains the key components of the Framework.

62. The Framework and its associated components are approved by, and are the responsibility of, the deposit taker – they are not approved by the Reserve Bank. The Strategy and Statement are reviewed and approved simultaneously by the board, supported by the overarching Framework to provide a complete view of risk management, as this ensures consistency, alignment and informed decision-making.

63. The Strategy for example does not have to be a standalone document and could form part of any Framework documentation but needs to be clearly defined if part of another Framework document We expect deposit takers to have a clear Strategy and Statement which they can successfully execute and articulate to stakeholders and decision-makers.

Notification requirements (Clause 15)

64. Clause 15 of the Standard includes a number of formal requirements relating to reporting and notification obligations, and deposit takers, are required to:

    64.1. Provide the Reserve Bank with, on adoption and following any material revisions, a copy of the deposit taker's Strategy and Statement. This must be provided as soon as practicable, and no more than 10 days, after approval by the board. Note that section 35(6) of the Interpretation Act 1999 would allow a deposit taker to provide the documents on the next available working day, should the 10th day fall on a non working day.

    64.2. Notify the Reserve Bank of material changes made to the Framework.

65. We expect that deposit takers are in regular dialogue with their supervisors about potential material Framework changes. Material changes to the Framework include changes relating to the substance of risk management, rather than changes relating to the format of document(s). Minor procedural changes are not considered material changes.

Subpart 3 Operational requirements (Clauses 16-28)

Setting risk management policies and processes (Clause 16)

66. Clause 16 of the Standard requires deposit takers to establish and maintain policies and processes that are aligned with the Strategy and Statement.

67. Policies and practices facilitate a consistent approach to the identification, assessment and management of risks by deposit takers. This ensures the deposit taker is being prudently managed, having regard to the size, nature of its business and complexity of its operations. The requirements, taken collectively, aim to help deposit takers manage risk effectively as well as improve decision-making and sound governance of deposit takers. Which particular risk management policies and processes are needed is best determined by the deposit-taker considering its size, nature and complexity.

Monitoring and notification procedures (Clause 17)

68. Clause 17 of the Standard requires deposit takers to have procedures for identifying, monitoring, and providing internal notification of risk exposures, risk issues, and any breach or non-compliance. Reports should provide accessible information at the right level, ensuring well-informed decision-making and efficient use of governance. This includes ensuring risk reports are clear, concise and easy to comprehend, with matters requiring discussion and decision clearly drawn out.

Use of models (Clause 18)

69. Clause 18 requires deposit takers to have policies and process aimed at identifying the limitations and assumptions relating to any models used to measure components of risk that could materially affect their decision-making. This is consistent with the approaches taken to managing model risk in the Capital and Liquidity Standards. We expect that these policies and processes would be applied to all models used to manage material risks in the deposit taker.

Examples

70. The requirement set out in clause 18 of the Standard is less relevant to deposit takers who do not use complex models to measure components of risk. For example, a Group 3 deposit taker might use a more basic approach to monitor credit risk and conduct stress testing than a larger deposit taker. In that case, a Group 3 deposit taker would be expected to still consider whether model risk poses a material risk to their operations, and consider an appropriate response.

Problem assets (Clause 19)

71. The Standard also requires deposit takers to have prudent and well-documented policies and processes for the early identification and management of problem exposures, including non-performing and restructured exposures. Early identification of a deterioration in loan quality or increasing problem exposures can improve options for remediating the exposure and managing the risk.

Contingency arrangements for stress conditions (Clause 20)

72. Clause 20 requires deposit takers to have policies and processes related to establishing and maintaining appropriate contingency arrangements to address risks that may materialise and actions to be taken in stress conditions.

73. Contingency arrangements, such as continuity and recovery planning, are designed to address unexpected stress events or risks and involve defining action steps to be taken if an identified risk event should occur, including addressing potential risks and their impact. These are important responses to risk and would be expected to be considered as part of the overall Framework.

74. As documented in the Operational Resilience Standard, a deposit taker is required to have board-approved business continuity plans (BCPs) that enable it to maintain its critical operations through defined tolerance thresholds in the event of an operational disruption.

Management of conflicts of interest (Clause 21)

75. Clause 21 requires deposit takers to have policies and processes related to managing conflicts of interest. We consider managing to include identifying and monitoring, and we consider conflicts of interest to include potential, perceived and actual conflicts.

76. As highlighted in clause 21(2) of the Standard, in particular, a deposit taker must have a clear policy setting out why and how a discretionary benefit that is linked to its financial performance may be provided to a person involved in a risk management function or a compliance and internal audit function for the deposit taker. This requirement is to avoid a discretionary benefit, such as a bonus, creating misaligned incentives for risk management, compliance or audit staff.

77. Policies and procedures on conflicts of interest support deposit takers to articulate what a conflict of interest is and, when an actual or potential conflicts of interest arises, ensures that the deposit taker has a process in place to identify, monitor and manage it.

Examples

78. A specific example of a potential conflict of interest relates to dual-operating groups. For entities with both a subsidiary and a branch operating in New Zealand (that is, entities operating two related licensed deposit takers), we expect that the conflicts of interest policies specifically address situations where the New Zealand Chief Executive Officer (CEO) of the branch is also an employee of the subsidiary, as well as potential conflicts of interest between related parties (both as part of ongoing risk management requirements and in a stress situation).

79. Further potential conflicts of interest could include some of the below, for example:

    79.1. financial incentives that potentially conflict with an individual's role;

    79.2. deposit taker directors sitting on boards of related entities – for example, a director responsibilities to one organisation could conflict with their responsibilities to another organisation;

    79.3. deposit taker staff and directors having personal financial investments, considering for example having investment in other operating entities which carry out business with their employer; and

79.4. senior management in the deposit taker having assigned responsibilities across different business areas with overlapping areas of interest.

80. In developing a conflicts of interest policy an entity should consider how it aligns with their Fit and Proper policy under Part 4 of the Governance Standard.

Reviews (Clause 22)

81. Clause 22 of the Standard requires annual review of the board-approved Strategy and Statement documents (the **annual review**), and a three-yearly comprehensive review of the overall Framework (the **comprehensive review**). Table 3 below details the main types of reviews for deposit takers to consider.

82. Reviews of the Framework, including its policies and procedures, can systematically identify deficiencies in the effectiveness of the programmes. This ensures the Framework is effective in identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating material risks.

83. Additionally, deposit takers may conduct the following reviews of the Framework:

83.1. **periodic reviews**: deposit takers may choose to review aspects of their Framework on a periodic basis, regarding for example a particular ongoing issue or material risk. These reviews are scheduled at regular intervals and typically planned for specific timeframes (quarterly, or annually). Their purpose is to ensure continued compliance, identify areas for improvement, and confirm that set objectives are met.

83.2. **event-based reviews**: an event-based review is triggered when a specific, significant event occurs, rather than at fixed periodic intervals and relying on a schedule. These reviews are important in providing deposit takers with key timely lessons learnt, gathered immediately after an event and helping to improve associated policies and processes for future events. For example, following a breach of risk limits, a significant deviation from policies, or following a 'material incident'.

Table 3: Reviews for deposit takers to carry out

Review type	Review focus	Review frequency	Who conducts the review	Requirement or best practice
Annual	Strategy and Statement	Every 1 year	Internal audit or another independent person (e.g. consultants)	Requirement
Comprehensive	Framework	Every 3 years	Internal audit or another independent person (e.g. consultants)	Requirement

Periodic	Continued compliance and meeting objectives	Planned for specific timeframes (quarterly, annually)	Risk management, compliance or internal audit as appropriate	Best practice
Event-based	Significant event	Following a significant event	Risk management, compliance or internal audit as appropriate	As determined by the deposit taker

Implementation of review recommendations

84. Our intent is that reviews not only systematically identify deficiencies in the effectiveness of the Framework and its elements but also that those deficiencies are addressed. Clause 22(2)(a) of the Standard requires deposit takers to implement recommendations in a timely manner as this ensures these documents are updated to reflect any changes in the business environment, industry trends and regulatory requirements.

85. We expect timeliness to be commensurate with the significance of the recommendation as well as accounting for the review cycle. For example, as a rule of thumb, we expect that any annual review recommendations are implemented before the next annual review cycle began to be considered 'timely' (an exception to this may be for example if a deposit taker is remediating a large technological change which would require more time to fully implement).

Conduct of reviews (Clause 23)

86. Clause 23 of the Standard requires that a review undertaken at a deposit taker must be conducted by a person with sufficient operational independence from the deposit taker's risk management functions.

87. We expect a deposit taker to consider the factors outlined below when determining a sufficient level of operational independence from the deposit taker's risk management functions for a proposed reviewer and confirming their suitability to conduct the proposed review(s):

    87.1. the managerial reporting line of the individual is independent from the associated business line(s) of the Framework being reviewed;

    87.2. the individual has sufficient capacity and resources to conduct the review(s); and

    87.3. the individual is suitably trained, possessing relevant experience and skills with sufficient authority.

88. We expect a deposit taker to take an appropriately graduated approach, commensurate to the significance of the review to be undertaken when assigning sufficiently operationally independent reviewers. Periodic and event-based reviews might warrant second-line or third party reviewers, subject to the significance of the review (e.g. a material event that triggers an event-based review could need an external reviewer).

What a comprehensive review covers

89. We expect the comprehensive review to include a comparison of the deposit taker's current practice against any identified better practice, including this Guidance. Where any gaps are identified, we expect the review to outline steps to address these differences or identify why changing current practice is not considered appropriate.

90. We expect a comprehensive review would include an assessment as to whether:

    90.1. the Framework remains appropriate for the deposit taker and the risks it faces;

    90.2. the Framework has been consistently implemented;

    90.3. there are appropriate procedures in place to ensure that the Framework addresses any new risks or changes to existing risks, including lessons learnt from risk incidents and near misses; and

    90.4. consideration as to whether the Framework is effective in providing appropriate, effective and timely information to inform decision-makers.

91. For a comprehensive review, a deposit taker may draw upon the conclusions of annual, periodic and event-based reviews conducted within the previous three-yearly cycle where the reviewer determines they remain relevant and applicable. For example, a deposit taker may choose to invest in periodic reviews on a rolling annual basis with the intention that they contribute to the next regularly scheduled comprehensive review. We expect that if the reviewer assigned to a comprehensive review relies on these other reviews that this does not diminish their responsibility for the quality and recommendations of a comprehensive review.

92. As set out in Clause 24, deposit takers are required to notify their board in relation to the results of a review of its Framework and any proposed adjustments (and an internal audit-led review of its Framework, as detailed in clause 30(1)(e)).

Regular stress-testing programmes (Clause 25)

93. Stress testing assesses the resilience of deposit takers to severe/extreme but plausible risks (e.g., severe economic downturns or major cyber attacks).

94. Stress testing gauges the potential impact on a portfolio or entity of hypothetical events and/or movements in a set of financial variables. It includes scenario analysis and sensitivity analysis.

95. Clause 25 of the Standard requires deposit takers (except for branches) to have a regular and forward-looking stress testing programme covering all material risks. For Group 3 deposit takers, stress testing is only required to be undertaken for credit, liquidity, and operational risk (including cybersecurity risk). Stress testing must be commensurate with the size and nature of business of a deposit taker, and the complexity of its operations.

96. The Reserve Bank has previously issued a set of key stress-testing principles as best practice to support deposit takers development of stress testing programmes. These principles are buttressed by some broader considerations relating to other material risk categories that are discussed here, and deposit takers may wish to consider these to the extent that they are appropriate for their business operations.

97. It will not always be the case that each material risk (or each risk category) requires its own stress test. In some cases, it may be more appropriate to supplement a stress test with an additional component or consider a scenario that affects multiple risks. For example, a deposit taker may conduct a credit risk stress test, and then overlay an operational risk (e.g., a cyber incident) and present results with and without the operational risk component. This would allow a deposit taker to assess both the marginal effect of a cyber incident and also the plausible scale of multiple risks manifesting simultaneously.

98. Clauses 25 and 26 of the Standard relate to deposit takers' internal stress testing processes ("entity-led stress tests") and are in addition to our programme of industry stress tests ("supervisor-led stress tests"). The Reserve Bank uses stress testing as a supervisory tool and as a mechanism to monitor the stability of the New Zealand financial system.

99. Clause 26 of the Standard requires deposit takers to report the results of stress testing to the board, with context explaining how the results would be expected to be interpreted, as well as to the Reserve Bank. Following stress testing, a deposit taker must consider how to integrate the results of the test into its decision making on the operation of its business, its risk management processes, and the assessment of its capital and liquidity levels.

100. The Capital and Liquidity Standards include requirements relating to stress testing. These could be met as part of a deposit taker's regular stress testing programme, or as a separate exercise. It is for deposit takers to determine which approach is more appropriate for their operations. For example, a deposit taker's Internal Capital Adequacy Assessment Process (ICAAP) may form part of its regular stress testing programme or be treated as a separate exercise. We expect that stress tests relating to credit and liquidity risks would be undertaken with higher frequency than stress tests for other risk categories (i.e., at least annually).

101. Clause 26 of the Standard also requires deposit takers to consider how to integrate the results of stress testing programmes into decision-making, risk management processes and the assessment of their capital and liquidity levels. We expect that the results of internal stress tests are used by deposit takers for risk management, capital and liquidity buffer setting and strategy and investment decisions. We expect this consideration to be appropriately documented. In particular, we expect that a deposit taker's board would use findings of stress tests as a key factor when reviewing the deposit taker's Strategy and Statement.

Examples

102. Clause 25 of the Standard notes that stress testing programmes may include multiple models. It is not necessary for a stress testing programme of a smaller or less complex deposit taker to include multiple models.

103. We expect that Group 1 deposit takers would lead their own scenario design, and build and use their own stress testing models of credit risk. Group 2 deposit takers are encouraged to lead their own scenario design and to develop credit risk models for key portfolios, but may make use of scenarios and loss rates (by portfolio) from past supervisory stress tests published by the Reserve Bank adapted to their businesses and asset quality metrics.[1] Group 3 deposit takers are also encouraged to lead their own

[1] The Reserve Bank typically publishes aggregate loss rates by portfolio at the conclusion of each of its annual supervisory bank solvency stress tests, for example here (p25): https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/publications/bulletins/2025/assessing-banks-resilience-to-geopolitical-risks-results-from-the-2025-solvency-stress-test-nov-2025.pdf.

scenario design, and make use of published stress tests. However, in the absence of designing their own scenarios, they may consider applying loss rates (by portfolio) directly from past supervisory stress tests published by the Reserve Bank. Group 3 deposit takers should discuss appropriate loss rates with their supervisors.

Adequate management of information and data (Clauses 27 and 28)

104. Effective management information systems provide appropriate information for decision-making and support business reporting (e.g. production of risk and compliance data and reports). These are a central tool to help mitigate and manage risk and ensure the institution has regular, accurate and timely information regarding its ever-evolving risk profile.

105. Clause 27 of the Standard requires deposit takers to establish and maintain information management systems that include risk data aggregation tools and reporting capabilities that enable it to identify, measure, evaluate, monitor, report on, control, and mitigate internal and external sources of risk.

106. We expect that this may include, for example:

    106.1. setting out appropriate and auditable documentation and record keeping requirements, providing appropriate information for decision making and support business reporting;.

    106.2. managing, communicating and reporting of risk issues and outcomes;

    106.3. assisting the deposit taker's management to appropriately monitor and manage different material risks; and

    106.4. being sufficiently flexible to support decision-making during periods of stress, when the deposit taker's risk profile may significantly and suddenly change.

107. Risk data aggregation capabilities and risk reporting practice must support the board and senior management in making appropriate risk-based decisions, for example with generated reports provided on a timely basis.

108. A deposit taker's management information system must provide appropriate information (i.e. risk reports) at each level of management and decision-making within the deposit taker, both under normal operating systems and in times of stress. Clause 28 of the Standard sets out what features a deposit taker's information management system must include to provide appropriate information that informs its decision-making and to support its business reporting. In order to comply with clause 28, we would expect a management information system to:

    108.1. produce appropriate risk and compliance data and reports;

    108.2. incorporate information that is relevant to decision-making;

    108.3. report accurate, reliable and timely information;

    108.4. allow a deposit taker to identify, assess and monitor business activities, existing and emerging risks, financial position and performance;

    108.5. allow a deposit taker to monitor the effectiveness of, and compliance with, its internal control systems and report any exceptions that arise; and

108.6. be reviewed regularly to assess the timeliness and relevance of information generated and the adequacy, quality, and accuracy of the system's performance over time.

109. We expect deposit takers to implement controls for ensuring data in information and reporting systems is sufficiently current, accurate and complete such that data quality is adequate for timely and accurate analysis and reporting of risk. Internal information and reporting systems are expected to be secure and supported by adequate business continuity and disaster recovery arrangements. As highlighted in the Operational Resilience Standard, it is important for deposit takers to manage their critical operations through potential business disruption events. For example, cyber attacks pose threats to the information and reporting system security arrangements of deposit takers, and inadequately implemented policies and processes for business continuity could ultimately undermine the deposit taker's safety and soundness.

110. We expect deposit takers to recognise that these systems and capabilities can also be a source of risk.

111. Typically, more manual processes may be observed in smaller deposit takers, considering for example the fixed costs associated with the digitalisation of processes and controls. We expect that this could potentially expose relatively smaller or less sophisticated deposit takers to a greater degree (and different type) of operational risk compared to larger or more sophisticated deposit takers, with less frequent monitoring and reporting of risk.

112. For example, having greater reliance on manual processes could mean less efficient processes in place for monitoring current and incipient risk sources as well as slower remedial response times during times of risk crystallisation. We expect that deposit taker Frameworks account for this by implementing robust risk assessments and mitigation strategies, by maintaining clear entity-wide communication chains and regularly monitoring operational risks to proactively prevent issues before they materialise.

113. Digitalisation enables the automation and replacement of manual processes and controls. This may reduce operational cost and human error. It may also increase efficiencies with the enabling of real-time risk monitoring, reduce reliance on legacy expertise and improve overall approaches to risk management with ultimately less potential amplifiers for a deposit taker during times of stress. Therefore, we expect reliance on manual processes to be reduced over time.

Examples

114. Ensuring effective information management systems are in place is an expected requirement relevant to all deposit takers.

115. A Group 1 deposit taker with greater resources at its disposal may have relatively more advanced and complex systems with more in-depth coverage for measuring, assessing and reporting on a deposit-taker-wide basis. Comparatively, a Group 3 deposit taker may have access to a relatively simpler setup for internal data and information management, with less advanced ICT systems and capabilities (e.g. produced compliance and data reports being relatively more qualitative in nature).

116. As well as considering entity size, the complexity of a deposit taker's operations would also be of great importance: the greater the complexity of business operations, typically then would be expectations for more complex data and information management

systems to comprehensively manage those complex business operations for the deposit taker.

Subpart 4 Internal controls and functions (Clauses 29-34)

Internal control structures (Clause 29)

117. A strong internal control framework, including independent and effective compliance and audit functions, is part of sound corporate governance and risk management.

118. Clause 29 of the Standard requires deposit takers to establish and maintain an effectively controlled and tested operating environment, with internal controls in place. We expect this to consider the risk profile of the deposit taker and take a forward-looking view.

119. The internal control framework must be reviewed as part of the annual audit plan.

Requirement for risk management function (Clause 30)

120. A risk management function is part of the second line and is responsible for supporting the board, relevant board committees and senior management in their roles in relation to risk management.

121. Clause 30 of the Standard requires deposit takers to have a dedicated risk management function. A key role of deposit taker's risk management function is to provide independent and objective review and challenge, oversight, monitoring and reporting in relation to material risks arising from the deposit taker's operations. We expect these risk management functions to cover all material risks and operate with;

    121.1. access and authority: to be involved in, and have the authority to provide effective challenge to, activities and decisions that may materially affect the deposit taker's risk profile.

    121.2. operational independence: to be separate from the risk-taking functions, with separate reporting lines.

    121.3. sufficient resources: having personnel who have clearly defined roles/responsibilities and experience/qualifications that meet the operational and compliance demands, and required ICT systems.

122. We expect that risk management is a discipline embedded throughout the organisation and that all staff within a deposit taker can support risk management functions. While it is common for risk managers to work closely with business units, the risk management function must be sufficiently independent. We expect deposit takers to determine what is sufficient resourcing for their risk management function, for example a smaller Group 3 entity may fulfil their needs with a single person depending on their size, nature and complexity of operations.

123. The Standard also requires that the risk management function be subject to regular review by the internal audit function, which may be part of the broader comprehensive review. Regular review brings objective, additional expertise and resources to the process of identifying, managing and controlling risks.

Chief Risk Officer (CRO) (Clause 31)

124. Deposit takers must have a CRO (or equivalent role). A CRO is accountable for risk management and oversees a dedicated risk management unit. CROs lead the second line, providing corporate leadership and ongoing monitoring to ensure risk exposures are within prudent risk limits. We expect CROs to also support the board in its engagement with, and oversight of the development of, the Strategy and Statement, which ensures that these documents are implemented through the deposit taker.

    124.1. With the CRO having responsibility for all risk types, they are well placed to present a comprehensive view of risks and highlight key issues requiring focus and visibility. CRO reports therefore can provide a key source of insight into an entity's risk profile.

    124.2. We expect there to be scope to consider the particular role appointment and any support or training offered by the entity to gain risk management expertise, consistent with the approach in the Governance Standard (including Fit and Proper requirements).

125. The appointed individual must have no other leading role in the deposit taker, although as highlighted in clause 31(3), the person appointed to oversee and manage the risk management function of a Group 3 deposit taker may have executive responsibilities that are separate from, and in addition to, the risk management function. Maintaining independence where pragmatically feasible regarding an executive's assigned responsibilities is important. For example, an executive would be expected to not have a conflicting function (for example, a CFO or CEO role) and should devote sufficient time to risk. We consider having a dedicated CRO represents best practice and would encourage Group 3 deposit takers to employ a dedicated CRO in situations where this is practical.

126. The Standard does not require the head of the risk management function to have the job title of "Chief Risk Officer", as long as they meet the requirements imposed on a CRO by the Standard.

127. Clause 31(2) sets out requirements for the independence of the CRO and specifies roles that cannot also be performed by the CRO. This is important to support a risk culture where the CRO and the risk management function can offer an appropriate level of challenge to the first line function.

128. Clause 31(4) requires that, if the CRO (or equivalent role) of a deposit taker is removed from their position for any reason, this must be done with the prior approval of the deposit taker's board. This gives the CRO some independence from the CEO and other senior managers while reflecting the nature of the role of the CRO as a senior manager who challenges management in relation to its risk management practices.

Requirement for compliance and internal audit functions (Clauses 32-34)

129. A compliance function is responsible for identifying, reviewing and monitoring a business' compliance risks (such as compliance with prudential requirements, ant-money laundering requirement, privacy law etc). The Standard sets out several requirements relating to compliance functions.

130. Clause 32 of the Standard requires deposit takers to have a dedicated, independent and adequately resourced compliance function. The structure of the compliance function is a

matter for the deposit taker. The Standard does not require the compliance function to be an organisational unit.

131. The risk management function may be combined with the compliance function, so long as the roles and responsibilities of each function are sufficiently allocated and resourced.

132. The compliance function cannot be outsourced by Group 1 and Group 2 deposit takers. However, they may engage the services of an external provider to perform certain select tasks that are part of these functions provided it is satisfied that each function as a whole meets the requirements of the Standard. Group 3 deposit takers and branches are permitted to outsource the compliance function or, in the case of branches, the compliance function may be resourced by the overseas deposit taker outside of its New Zealand operations.

Internal audit function

133. Clause 32 of the Standard also requires deposit takers to have an independent and adequately resourced internal audit function. The internal audit function (the third line), in the context of the Standard, is responsible for carrying out audits and providing the board and senior management with assurance that the business is managing risk appropriately. More broadly, clause 33 of the Standard sets out that deposit takers must ensure respective risk management, compliance, and internal audit functions are all adequately resourced with suitably experienced and qualified persons.

134. An internal audit function's responsibilities include assessing whether existing policies, processes and internal controls (including risk management, compliance and corporate governance processes) are effective and appropriate.

135. Clause 34 of the Standard sets out that under its internal audit function, a deposit taker is required to prepare an annual audit plan to ensure compliance with its policies and processes. The process for developing, reviewing and approving an integrated audit plan should be clearly documented. This includes defining the roles and responsibilities of the three lines, senior management and the board audit and risk committees in the process.

136. The Standard does not require the internal audit function to be an organisational unit, however we do expect this function to be at least partially staffed by qualified auditors, according to the individual deposit takers' needs. In particular, it is common for internal audit to be a separate organisational unit to compliance in a deposit taker.

137. A deposit taker must not have one appointed executive with assigned responsibilities spanning all of risk, compliance and internal audit. In practice a smaller entity with lesser available resources may have one person responsible for risk and compliance, however this individual would not have assigned responsibility over the internal audit function as this function must remain independent of a second line function.

138. The internal audit function cannot be outsourced by Group 1 and Group 2 deposit takers. However, they may engage the services of an external provider to perform certain select tasks that are part of these functions provided it is satisfied that each function as a whole meets the requirements of the Standard. Group 3 deposit takers and branches are permitted to outsource the internal audit function or, in the case of branches, the internal audit function may be resourced by the overseas deposit taker outside of its New Zealand operations so long as they meet the requirements of the in clauses 32-24.

Subpart 5 Organisational responsibilities and practices (Clauses 35-37)

Responsibilities of boards and senior management (Clauses 35-36)

139. The board of a deposit taker is ultimately responsible for risk management. Clause 35 of the Standard supports this by placing requirements on a deposit taker for its board to carry out specific responsibilities. Responsibility for the management of a deposit taker's business operations would be expected to rest with its board, and this includes the entity's Framework. This aligns with the approach in the Governance Standard.

140. We do not however expect the board to be involved in the day-to-day management of risks. Responsibility for the operation of a deposit taker's Framework is required to be with senior management as they are responsible for operationalising the monitoring and management of risk, including the monitoring and managing of all material risks consistent with the board-approved the Strategy and Statement, as detailed in clause 36 of the Standard.

141. 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. 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.

142. Requirements for board responsibilities apply equally across all deposit taker groups given their fundamental importance. Risk Committee.

143. For further information and details regarding board responsibilities, refer to the Governance Standard.

Risk culture (Clause 37)

144. Risk culture refers to the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify, understand, openly discuss and act on the organisation's current and future risk. Not only does a sound risk culture, promote risk awareness and support ownership and accountability for risk management, but it importantly also enables the implementation of timely and appropriate action when issues arise or when risks move outside established thresholds.

145. Maintaining a strong risk culture relies on a deposit taker understanding the material risks it takes and ensuring there are frameworks in place which best support the most effective way of proactively identifying, assessing and mitigating those risks. Our view is that sound culture is a critical feature in effective risk management practice and is important in ensuring that risk management processes are not seen as a compliance or 'tick box' exercise.

146. Clause 37 of the Standard requires the board to encourage a sound risk culture throughout the deposit taker to promote the development and execution of its Strategy. A deposit taker's risk culture is strongly influenced by the board and therefore we expect the board to take responsibility for a deposit taker's risk culture. We expect that the Board would have a view of the risk culture that is appropriate for ensuring that the institution operates within the risk appetite.

147. We expect the board and senior management to demonstrate their commitment to risk management and foster a sound risk management environment in which staff are actively engaged with risk management processes and outcomes, and a risk management function that is influential and respected.

148. A mature sound, and adequate risk culture is one where staff at every level have an understanding and appreciation of the aims of risk management and appropriately manage risk as an intrinsic part of their day-to-day work. When an organisation has a poor risk culture, they either have failed to set appropriate frameworks and have adequate policies and processes to address risk, or they have failed to embed those frameworks within the organisation.

149. We expect all entities to establish a proactive, rather than reactive, risk culture to best ensure that they can respond in a timely manner to the emergence of risk(s) with efficient remedial programs, where required.

Examples

150. Table 4 below provides some illustrative examples of how deposit takers can demonstrate good risk culture, as well as examples of behaviour and culture that are not conducive for enabling and maintaining sound risk management practices.

Table 4: behavioural and cultural indicators of deposit taker risk culture

Behaviours and practices demonstrating and enabling good risk culture	**Behaviours and practices** demonstrating and enabling poor risk culture
• Ensuring all persons within the institution have an awareness of the Framework and developing an appropriate risk culture across the deposit taker. This includes having a documented and shared understanding of the deposit taker's risk appetite and target maturity.	• Pursuing a business strategy that prioritises growth without ensuring appropriate management of risks.
• Having clearly defined roles, responsibilities and lines of authority for risk management procedures.	• Inadequate or unclear communication regarding acceptable and unacceptable activities/behaviours. Also, roles and responsibilities not correctly/clearly set out – resulting in unclear role delineation and expectations and insufficient capabilities, which could produce poorly developed controls, inadequate monitoring and reporting, and perverse incentives.
• Encouraging and educating others in risk and risk management to promote the effectiveness of internal controls and risk reporting. This could be through for example focused training efforts and regular communication from the board to all relevant staff.	• Staff do not feel empowered to openly raise concerns to leaders and fear reprisal. There is not a 'speak up' culture, and there is the absence of positive incentives being in place.
• Supporting transparency of risks, events and issues, and facilitating effective internal controls and risk reporting. For example: setting key performance indicators requiring regular ongoing training, audits of training effectiveness, ensuring there is sufficient resourcing and capacity to undertake training. Also, ensuring risk management systems	• Risk indicators that remain 'red' for extended periods of time could indicate complacency or a lack of resource or focus in the overall management of risk.

Behaviours and practices demonstrating and enabling good risk culture	**Behaviours and practices** demonstrating and enabling poor risk culture
incentivise behaviours that are consistent with good practice and disincentivise or address those consistent with poor practice.	
• Achieving "buy-in" at all levels of the deposit taker as to the value of risk management.	• Risk management systems fail to adequately capture and report risks. Outstanding audit items are not addressed or ignored.
• Demonstrating a positive attitude towards risk management by raising risk as part of every decision and rewarding staff who proactively identify risk issues early.	• Inadequate consideration of the resources and capability required to both administer the Framework and ensure ongoing compliance.
• Routinely providing the board and senior management with clear and easily understandable information on the deposit taker's material risk exposure such that the board and senior management obtain sufficient information to understand the nature and level of risk being taken by the deposit taker, and how this risk relates to adequate levels of capital and liquidity.	• Only positive news is shared with the board and senior management. This could result in boards setting aside less dedicated time for reviews and discussions, and ultimately there being less active challenge offered.
• Taking appropriate actions in a timely manner for any breach or non-compliance issues.	• Reporting only covers breaches, with little discussion of the overall risk profile at board level. This could potentially delay the identification and management of heightened risks.