RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Summary of submissions:
Risk management guidance on cyber resilience and views on information gathering and sharing

April 2021

Contents

Background

1. In October 2020, the Reserve Bank of New Zealand - Te Pūtea Matua published its consultation document and the draft *Guidance on Cyber Resilience* to invite feedback on the guidance and initial perspectives on information gathering and sharing. This followed our announcement that we would take a more proactive role in promoting financial sector cyber resilience in the November 2019 *Financial Stability Report*.

2. After considering all of the submissions we received and consulting with experts from the National Cyber Security Centre (NCSC), we have revised and finalised the *Guidance on Cyber Resilience*. This non-binding guidance will apply to all entities regulated by the Reserve Bank, including banks, non-bank deposit takers, insurers and financial market infrastructures.

3. We also received constructive feedback on developing the information gathering and sharing plan. We have summarised the key principles we will follow when developing the plan and we expect to publish it later this year for public consultation.

Consultation process

4. The consultation "Risk management guidance on cyber resilience and views on information gathering and sharing" opened on 20 October 2020 and closed on 29 January 2021.

5. On 9 December 2020, we held a workshop for the industry and invited the NCSC, Computer Emergency Response Team (CERT NZ), and the Financial Market Authority (FMA) to the workshop. Around 30 participants attended in person and more than 90 participants attended online. During the workshop, we introduced the draft guidance on cyber resilience and introduced our initial thoughts on information collection and the collaborative approach we take to promote cyber resilience together with the NCSC, CERT NZ and the FMA. The three agencies also introduced their roles in promoting cyber resilience of the financial sector.

6. We received 16 submissions on the consultation paper, comprising:

   - One submission from a bank - Bank of New Zealand;
   - Four submissions from stakeholder groups - Financial Service Council, Financial Services Federation, Insurance Council of New Zealand, and New Zealand Bankers Association;
   - Three submissions from payment or settlement system operators - CLS, Mastercard, and Payments NZ;

- Five submissions from insurance companies - Cigna Life Insurance New Zealand, Fidelity Life Assurance Company Limited, NIB NZ, Southern Cross Health Society, Swiss Re Life & Health Australia Limited; and
- Three submissions from service providers - Amazon Web Services, Datacom, and Microsoft.

These submissions have been uploaded to the Reserve Bank website except for those submitted by the Bank of New Zealand and NIB NZ who requested that their submissions remain confidential.

Reserve Bank's role and policy stance

7. All submissions acknowledged the Reserve Bank's role in promoting cyber resilience amongst its regulated entities. Several submissions mentioned that the *Guidance on Cyber Resilience* outlines priority areas for improving cyber resilience and is expected to improve cyber resilience capabilities in the financial sector.

8. Most submissions supported the Reserve Bank's policy stance of being moderately active. However, some suggested making the requirements legally binding, which they consider more effective to change underlying behaviours and warranted by the significant threats that cyber attacks pose to the financial system.

9. We acknowledge the potential benefits of taking a more stringent approach –issuing legally binding requirements to promote cyber resilience. However, we confirm our policy stance of being moderately active and publishing non-binding recommendations by taking into account the following three aspects:

   - The history of the Reserve Bank's policy stance on cyber resilience - compared to the Reserve Bank's previous light-touch approach regarding cyber resilience, issuing non-binding guidance is a reasonable starting point before taking a more stringent approach;
   - Providing the industry sufficient time to adjust to new policy settings around building cyber resilience - considering the variety and diversity of financial institutions in New Zealand (size, services, resources and home jurisdiction requirements) there is a wide range of maturity towards cyber resilience. More generally, there is also a significant gap between New Zealand and jurisdictions with sophisticated cyber readiness[1]. We intend to use the forthcoming cyber information collection as a tool to help measure the effectiveness of non-binding guidance and guide future policy setting (such as developing legally binding standards for cyber resilience);

[1] The International Telecommunication Union, Global Cybersecurity Index version 4, 2021

- The resources available to monitor and ensure compliance – we are looking to strengthen our cyber resilience expertise in our financial stability function, but this will take time to achieve. Taking a moderately active approach is a feasible choice that sets the foundation for future advancement.

10. As suggested by some submitters, being moderately active is a starting point for future policy development. We will work together with the industry to operationalise the finalised guidance, and will continue our on-going engagement to strengthen cyber resilience.

11. One submitter did prefer that we took a more active role in promoting cyber resilience. However, the submitter noted that, given the maturity of cyber resilience in the financial system of New Zealand, taking a highly active role may not be the most suitable approach when commencing a regulatory regime. This is consistent with our analysis.

12. Another submitter suggested that we should partner with industry-neutral central advisers to build and maintain cyber resilience guidance. That is the approach that we adopted when developing the *Guidance on Cyber Resilience*. The NCSC, as the national level expert on providing NZ's most significant organisations to protect their information systems from advanced cyber threats, has provided valuable feedback on the draft guidance. We will continue to drawing on the expertise of pan-sector cyber resilience organisations like the NCSC and CERT NZ to maintain the guidance and for future policy development.

Guidance on cyber resilience

13. The confirmed *Guidance on Cyber Resilience* has been published alongside this summary of submissions. This part summarises the feedback we received and how we have integrated the feedback into the guidance. The Appendix to this document provides a comprehensive summary of our responses to all feedback on the text of the *Guidance on Cyber Resilience*.

Enforceability and implementation of the guidance

14. Some entities asked for clarification about the enforceability of the guidance. We would like to make it clear that the guidance is a set of recommendations rather than requirements. This means the guidance is non-binding and is not intended to be used as a checklist for compliance.

15. Some international financial institutions which are subject to laws in their home jurisdictions (or subject to the oversight of cooperation arrangements) asked for an exemption from the guidance. We do not consider such exemptions as necessary. As noted earlier, the guidance does not have a legally enforceable status. However, as the guidance is aligned with international standards, financial institutions may find that their practices meet the recommendations outlined in the guidance if they have adopted international standards in their cyber risk management. Since our guidance is more recent than some international standards, some content may be worth consideration for international institutions (e.g. recommendations about outsourcing to cloud computing service providers and recommendations on information sharing).

16. Some entities asked the Reserve Bank to provide an implementation timetable for the guidance. Implementation of the guidance will ultimately be integrated with our broader programme of work around building cyber resilience, which includes the development of a cyber data collection plan and efforts to better coordinate system-wide responses to cyber incidents. These are both longer term objectives. In the nearer term, we will integrate the guidance in our supervision engagement with our regulated entities. Regulated entities are expected to proactively consider how their current approach to cyber risk management lines up with the recommendations outlined in our guidance and look for gaps for improvement as early as possible, since strengthening cyber resilience needs holistic planning as well as requiring sufficient time and resources to implement and to see notable improvements.

Alignment with international standards

17. All submitters supported the Reserve Bank sticking closely to international practices in developing the *Guidance on Cyber Resilience*. One entity suggested that we map back the guidance to international standards to allow entities to leverage the work they have done to comply with other standards. We have chosen not to do so because the guidance is a set of high-level recommendations rather than a checklist of binding requirements. We acknowledge the potential convenience that mapping the guidance to international standards may bring to some entities. However, considering the variety of entities that the guidance will apply to and the variety of international standards, we have left space for our regulated entities to decide the most suitable way to check how their current efforts and practices align with our guidance.

18. One entity suggested that we adopt the Australian Prudential Authority's (APRA) approach to publish much shorter high-level standards (like CPS234) supplemented by more detailed guidance (like CPG234). We acknowledge the benefits of adopting a similar approach but would like to emphasise that ARPA's approach reflects an evolution in its policy development, which began with guidance and then moved to legally binding standards at a later stage. APRA's approach has evolved with the maturity of cyber resilience of the financial sector in Australia, as well as the increased resources and expertise in APRA in cyber resilience.

Pan-sector guidance and the principle of proportionality

19. All submitters supported that the guidance be applied to all entities regulated by the Reserve Bank. Some submitters stated that smaller financial institutions will especially benefit from the guidance as a roadmap to help increase their capacity for cyber resilience.

20. All submitters agreed that the principle of proportionality should apply across the guidance. One submitter stated that the size of a financial institution should not be a major factor in a risk-based approach. As covered in the consultation paper, a lot of factors affect how an entity should aim to improve its cyber resilience and how the regulator will have different expectation on different entities. The size, structure and operational environment of an entity, as well as the nature, scope, complexity and riskiness of the products and services provided by the entity all play a role here. Size is only one factor, rather than being regarded as the major factor.

21. Generally, large financial entities, which have more customers, provide more diversified and complex products/services and are more interconnected with other financial institutions, should target a relatively higher level of cyber resilience compared to smaller and less complex entities. One example is domestic systemically important banks (D-SIBs); another example is designated financial market infrastructures. However, publishing a list of entities that will be subject to the enhanced level of expectations by the regulator may overlook the fact that some relatively small entities do provide complex services, or may have channels that are more exposed to cyber risk. Therefore, we will not be drawing a threshold above which the enhanced level of expectations applies. An entity should be able to determine the appropriate level of cyber resilience it wants to achieve according to the previously mentioned factors and make sure the chosen level of cyber resilience is aligned with its overall business strategy.

22. One submitter asked for more room to scale down the guidance considering that small financial institutions may have less inherent cyber risk compared to large financial institutions. They argued that small entities lack resources to implement the guidance "to its full extent." The non-binding and risk-based nature of the guidance means that entities should not use the guidance as a minimum checklist. However, some recommendations outlined in the guidance, for example, those on governance, are expected to be closely followed by all entities regulated by the Reserve Bank. The supervisory engagement will provide more clarity about the expectations of different entities.

Level of detail in the guidance

23. All submitters supported the guidance being pitched as high-level and principles-based, allowing it to remain flexible so it can address the increasingly dynamic complexities in the financial and technology spaces. However, there are some differences of opinion about the level of detail specified in the guidance. Some submitters thought that more details were needed so that the guidance could better target the board and the senior management of organisations, especially for those entities which lack expertise in managing cyber risk. In contrast, some thought that the guidance was too detailed and prescriptive.

24. When developing the guidance, we tried to strike a balance between providing sufficient details and being too prescriptive. The guidance is intended to provide an appropriate level of detail to allow the guidance to be a stand-alone document and avoid being too lengthy or too technical. The guidance is not written for technical experts, and is instead focused on raising awareness for all staff, with either in-house expertise or independent organisations helping the board and senior management understand cyber risk. Should more detailed information be needed, well-recognised international guidance and standards (as listed in the Appendix of the *Guidance on Cyber Resilience*) will be the main sources to refer to.

25. Some submitters suggested that the guidance should emphasise a 'results-focused' approach. We understand the importance of driving behaviour change to achieve desirable results. The guidance does include results that the entities are expected to achieve (e.g. a sound governance structure and arrangement). However, similar to the discussion of the appropriate level of detail for the guidance, we are seeking to provide high-level guidance on how to achieve the desired outcome. The suggested content of a sound cyber resilience framework (A2.1.1 of the *Guidance*) is a good example.

26. As for the comments regarding some specific items in the guidance that were regarded as "too prescriptive" by some submitters, we have reviewed the wording and explained why some revisions have been taken on board, and why some have not. See the attached Appendix for more details on this.

Views on information sharing and gathering plan

27. All submitters supported our intention to follow international practices and establish data collection on cyber resilience. As outlined in the consultation paper, the information collection is planned to include two components: cyber incident reporting and surveys on cyber risk management capabilities. The detailed plan for information sharing and gathering is under development and our intention is to consult stakeholders later in the year. We have outlined the key areas that we will consider when developing the information collection plan, which includes the feedback we received from the workshop held on 9 December 2020 and from the submissions in response to our consultation.

Key areas for developing information sharing and gathering plan

Take a coordinated approach and avoid duplication

28. All submitters supported our plan to take a collaborative approach when developing our information gathering and sharing plans. We aim to minimise compliance costs associated with reporting on cyber resilience by collaborating and coordinating our efforts with relevant agencies such as the NCSC, CERT NZ and the FMA. These agencies have relevant expertise to support our data collection initiative and are key stakeholders in our broader planned efforts around improving the collective response to cyber threats and incidents.

29. Some submitters suggested it would be ideal to have a single reporting point, simplified breach reporting requirements, and to align notification timelines, templates and engagement process across government agencies to reduce duplication. We commit to working with the community of public bodies relevant organisations to see if it is feasible to integrate the different needs of agencies around breach reporting as much as practically possible. As each regulator has a different responsibility, it is potentially more challenging to have a single reporting point for breaches. For example, the privacy breach reporting requirement for the Office of the Privacy Commissioner (OPC) focuses on potential harms caused by privacy breaches, and this is likely to have very limited overlap with the cyber incidents reporting requirements for other agencies.

30. Some submitters mentioned the important role of information sharing platforms they are currently involved in both domestically and internationally (e.g. New Zealand Internet Task Force, the NCSC-sponsored Finance Security Information Exchange), and encouraged the Reserve Bank to leverage the existing forums when promoting information sharing. We also acknowledges that some entities, especially some payment/settlement operators, have been playing an active role in promoting the exchange of information about cyber resilience. As outlined in Part C of the *Guidance on Cyber Resilience*, we encourage entities to participate in reliable information sharing platforms and does not

intend to replace or duplicate any efforts in the existing information sharing channels. The ultimate purpose of our information collection is to monitor systemic risk and promote financial stability.

Clearly define the benefits of information collection and future usage of the information collected

31. Quite a number of submitters stated that they would like to get more clarity about the benefits of the information collection plan. The potential benefits include, but are not limited to, defining benchmarks that entities can aim for, promoting better and more coordinated responses to cyber incidents, and informing further policy development (i.e. to explore the necessity of having more stringent requirements in future). We will elaborate on the benefits of information collection and how information collected will be used to strengthen cyber resilience when the detailed plan is published for public consultation.

32. The primary purpose of the cyber data collection is to help us monitor the development of cyber risk in the financial system. The data collected is intended to both inform our own response to cyber incidents, and also support coordinated monitoring efforts with other government agencies. For example, we may consider analysing data about the financial sector's cyber landscape, and periodically publish summarised analysis. The information may also be used to promote supervisors' work, raise awareness of the importance of cyber resilience and encourage regulated entities to strengthen their capability. We fully agree with the sentiment from one submitter, who suggested that collecting information should aim to improve cyber resilience overall rather than being solely for statistical purposes.

Protect anonymity

33. Information about cyber incidents and cyber risk management are highly sensitive. One submitter suggested that we should encourage sharing lessons learned from cyber incidents in a consultative and demonstrative way, as opposed to under threat of punitive penalty or reputational exposure.

34. To encourage entities to share sensitive operational and technical security information, and avoid embarrassment and potential reputational damage when sharing details of compromised cyberattacks, we will keep information collected anonymous.

35. We will clarify the extent to which certain types of information collected will be shared with relevant government agencies, the industry and the public when we publish the information collection plan for public consultation.

Ensure information security and integrity

36. We will prioritise the security and integrity of information collected and will develop detailed plans to ensure that the confidentiality and the sensitivity of information reported by its regulated entities is properly protected. We will be transparent about how we manage, store and protect information collected. The recent illegal data breach of a third party file sharing application used by the Reserve Bank is a timely reminder of the risks associated with managing and sharing information. The KPMG review of our processes following the breach (to be released soon) has provided valuable lessons to us. This has resulted in a number of process improvement recommendations with many of these now underway.

Compulsory reporting on material cyber incidents

37. The first work stream on information collection is to design a detailed framework outlining requirements on cyber incident reporting. All submitters supported compulsory reporting about material cyber incidents with a clearly defined threshold of materiality. Following international best practices, we intend to follow a principle-based definition of materiality rather than using specific numerical measures. We will develop the reporting requirements with the definition of materiality, the reporting time frame and a detailed reporting template for public consultation.

38. For the reporting timeframe, we are aiming to strike a balance so that we are informed about the cyber incident in a timely manner and regulated entities will still have get sufficient time to evaluate the impact of an incident and focus on a quick response.

Survey on cyber capability building

39. Submitters generally supported our plan to conduct infrequent periodic surveys on cyber risk management practices of the regulated entities. The surveys will be mainly quantitative based to enable aggregation, bench marking and comparison. It is not intended to duplicate any existing internal/external audit by regulated entities.

40. As suggested in one submission, the frequency of the surveys will be proportional (e.g. more frequent (for example, once a year)) for large financial institutions but less frequent for relatively smaller entities.

Other considerations and suggestions

41. Submissions we received also covered aspects that are not directly related to the consultation paper or the guidance, but are very useful for us when considering the evolution of its policy in future to promote cyber resilience. The suggestions included dealing with any cybersecurity talent shortage, cross-sector co-ordinated cyber incidents response simulation exercises and red-team testing, and better cyber threat intelligence management and sharing.

Next steps

42. We will work with regulated entities to operationalise the published *Guidance on Cyber Resilience* by integrating the guidance into its supervision activities. The guidance will be used as a structured template to guide supervisors' engagement with regulated entities. Regulated entities are expected to follow the recommendations in the guidance in order to identify gaps and strengthen cyber risk management.

43. We will publish the information collection plan for public consultation later this year. We welcome feedback and will work together with the industry and relevant government agencies to promote cyber resilience in the financial sector.

Appendix: Summary of responses to the draft *Guidance on cyber resilience*

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Guidance—Part A: Governance	Suggest elaborating on the benefits of governance for risk management and setting up links between Part A and the other three parts.	The preamble of Part A emphasises the importance of governance as a foundation for good cyber risk management. The Reserve Bank acknowledges that governance is required throughout cyber resilience capability building. Some international standards embed governance in each section of capability building. However, we regard this only as a drafting style preference.	A paragraph is added to the end of the preamble of Part A to emphasise the overarching role of governance in each step of strengthening cyber resilience.
Guidance—Part A: Governance	The term of 'strategy', 'framework' and "implementation plan" should be clearly defined.	The definition of cyber resilience strategy is provided in the glossary of the draft guidance. The Reserve Bank agrees that a clear definition of cyber resilience framework should also be provided. However, we regard 'implementation plan' as a more generic term.	The definition of 'cyber resilience framework' is added in the glossary.
Guidance—Part A: Governance_ A1. Board and Senior Management Responsibilities	A1.4 The responsibility should remain within the remit of senior management rather than the board to ensure all staff with cyber resilience related roles and responsibilities are qualified to perform their roles and are informed and empowered to act in a timely manner.	'All staff' includes the senior management of an entity as well as other staff. Generally, senior management is responsible for ensuring other staffs' competency and the provision of resources needed to build cyber resilience within an entity. In addition, the board must ensure senior management are responsible for cyber resilience should be qualified and have resources to fulfil their tasks.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Guidance—Part A: Governance_ A1. Board and Senior Management Responsibilities	A1.6 The board of an entity should not be expected to approve matters such as the procedures and controls necessary to support the cyber strategy and framework. These should be left to management.	We agree that the board of an entity should be focused on strategic decisions including approving cyber strategy and framework. Supporting policies, procedures and controls remain the remit of management of an entity. The board of an entity should oversee implementation of its cyber framework, including policies, procedures and controls.	A1.6 is revised as 'The board should be responsible for approving the entity's cyber resilience strategy and framework, and monitoring the entity's implementation of cyber resilience framework, including policies, procedures and controls that support the implementation.'
Guidance—Part A: Governance_ A1. Board and Senior Management Responsibilities	A1.7.1 The word 'budgeting' should be removed to focus on 'plan'.	The focus of this recommendation is to ensure sufficient resources are planned and allocated to build cyber resilience. Sufficient resources should be reflected in the budgeting plan of the entity. The emphasis on budgeting does not indicate that an entity should only prepare a budgeting plan without preparing relevant action plans. As stated in A1.7, all relevant information should be updated to the board.	No changes made.
Guidance—Part A: Governance_ A1. Board and Senior Management Responsibilities	A 1.8 should make it clear that the appointed senior executive (e.g. Chief Information Security Officer) is 'accountable for' rather than 'take care of' cyber resilience issue.	We agree that the roles and responsibility of the appointed senior executive (e.g. CISO) need further clarification. While the Board of an entity is ultimately accountable for the cyber resilience of an entity, the CISO's responsibility is focused on the implementation level.	A1.8 is merged in A1.3.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	The appointment of CISO should belong to the remit of senior management, rather than the board.	We do not agree that appointing CISO should only belong to the remit of senior management. Globally, corporate boards are increasingly aware of cyber risk and increase their oversight. There is a trend that more 'board-appointed CISOs' comes into play.	
Guidance—Part A: Governance_ A1. Board and Senior Management Responsibilities	A1.8.1 It is not unusual in New Zealand for CISOs to be a member of the IT/operation department. The guidance should be outcome-focused to ensure a clear line of communication to the board for cyber resilience issues.	Although ideally the appointed senior executive responsible for cyber resilience should act independently from the IT/operation function of an entity, we acknowledge the fact that the appointed senior executives in some financial institutions are members of the company's IT team. The focus of this recommendation is to ensure that any issues/concerns observed by CISO can be reported to senior management and the Board directly. Therefore, we agree that we should provide flexibility for entities governance structure and focus on communication channels related to cyber resilience.	A1.8.1 is revised as 'The board and senior management should ensure the appointed senior executive be able to report observance/issues of the cyber resilience of the entity to its senior management and the Board directly' and is re-numbered as A1.3.1.
Guidance—Part A: Governance_ A1. Board and Senior Management Responsibilities	A1.8.2 should be revised to recommend the internal audit team remains independent, noting CISOs are likely to be involved when attending meetings with internal audit during fieldwork, validation and reporting stages.	The internal audit team should be independent when reviewing the cyber resilience of an entity. We acknowledge that the appointed senior executive will be required to attend meetings during the internal audit process but should never be involved in assessing and evaluating the cyber resilience of an entity as part of the internal audit team or interfere with internal audit's assessment.	A1.8.2 is revised as 'The appointed senior executive should not interfere with the entity's internal audit on the cyber risk management of the entity' and is re-numbered as A1.3.2.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Guidance—Part A: Governance_ A2. Cyber Resilience Strategy and Framework	A2.1.1 The suggested contents of the cyber resilience strategy are too prescriptive and needs to be higher level. The word 'should' should be replaced by 'could' to enable entities themselves to develop strategy and framework that are commensurate with their vulnerabilities and exposure to threats. Should add the details of 'confidentiality, integrity, availability' to the stakeholders' high-level requirements in cyber strategy. The mission (i.e. goals) should set the cyber resilience strategy of an entity, rather than setting the missions within the strategy.	The guidance aims to strike a good balance between being too detailed and being too high-level. The suggested contents are on a sufficiently high level to give entities recommendations about what a cyber resilience strategy should include. Since the Guidance is non-binding and the recommendations are based on observed industry good practices, it is not necessary to revise 'should' to 'could' in the wording. The preamble of Part B (Capability Building) covered the relevant contents about maintaining the confidentiality, integrity and availability of information assets. The reason for not including relevant details in A2.1.1 is to leave space for entities to design their own cyber resilience framework according to the unique requirements of their stakeholders besides the common goals mentioned above. Entities should follow the guidance to draft their cyber resilience strategy according to their size, service and nature, reflecting any common or unique requirements from their stakeholders. Missions should be reflected in the cyber resilience strategy of an entity. A2.1.1 reads 'The cyber resilience strategy should outline...the entity's vision and mission regarding cyber resilience; ...' It does not mean the mission is set within the strategy.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Guidance—Part A: Governance_ A2. Cyber Resilience Strategy and Framework	A2.5 'Internal audit' should be replaced by 'independent assurance' considering limited skillset the internal audit team may face, especially for small banks.	The Reserve Bank acknowledges that the internal audit team of some financial institutions may have limited skillset on cyber resilience and face resources constraint to carry out cyber resilience related internal auditing tasks. However, the word 'internal audit' does not mean that the internal audit team cannot employ external expertise when carrying out internal auditing.	A2.5 is added with the following sentence 'The entity should ensure the independence of its internal audit team either by using its in-house internal audit capability or external resources'.
Part A: Governance_ A3. Culture and Awareness	A3.1.1 Sharing relevant information about the cyber resilience strategy and framework with all staff of an entity should be sufficient, rather than sharing the entire framework.	The purpose of A3.1.1 is to build a culture of cyber resilience for all staff of an entity. The entity should decide the level of detail it shares about the cyber strategy and framework with staff in different roles and responsibilities. This is to ensure that the necessary information is delivered to all staff without compromising the sensitivity of certain information contained in an entity's cyber resilience framework or implementation plan.	A3.1.1 is revised as '... should include sharing relevant information of the cyber resilience strategy and framework to all staff'.
Part A: Governance_ A3. Culture and Awareness	A3.2.1: Specific cyber threat intelligence can only be shared with key stakeholders rather than business-wide.	This recommendation does not limit financial institutions' capability in deciding the level of detail and the range of cyber threat intelligence that are shared with staff for the purposes of building culture and awareness.	A3.2.1 is revised as 'The entity should… and share as appropriate with staff to aid in business-wide situational awareness'.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part A: Governance_ A3. Culture and Awareness	A3.3 The capability of providing training could be either delivered from within the entity or external resources.	As per A2.5, the Reserve Bank acknowledges that some small entities may not be able to maintain a programme for continuously training staff and raise awareness on cyber resilience. An entity should decide whether to deliver the training using in-house resources or refer to external sources as long as the training meets the requirements of the entity.	No changes made.
Part B: Capability Building_B1. Identify	B1.2 and B1.3 may cause the confusion that an entity needs to maintain its inventories and network maps as separate documents.	B1.2 and B1.3 do not intend to suggest that the inventories and network maps need to be maintained in separate documents. Similar to what has been stated in the preamble of Part A: Governance ("The cyber resilience strategy and framework can be standalone files or well embedded in an entity's other strategy and framework") the guidance gives flexibility for entities to decide where and how they keep the inventories and network maps.	No changes made.
Part B: Capability Building_ B2. Protect	B1.5 What does 'holistic self-assessment' constitute, and would red team testing, penetration testing, and vulnerability scans meet the intention?	Risk assessments refers to a very broad range of practices and is not limited to testing. The Reserve Bank agrees that "holistic self-assessment" needs further clarification and regards "risk assessments" as more appropriate in the context.	B1.5 "a holistic self-assessment" is revised as "risk assessments".

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part B: Capability Building_ B2. Protect	B2.2. It is too specific to require segmentation. Segmentation is one of the mitigants to cyber-attacks, but there are a number of others. Segmentation could be included, along with some other approaches, as examples of boundaries. Networks are progressing towards the concept of zero trust (network, data, identification, and device segmentation and management) with the focus on protecting information, not network segments.	The intention of B2.2 is to recommend entities to adopt an effective approach to protect their data and systems. The Reserve Bank acknowledges the advancement in mainstream technologies deployed by entities to mitigate risks (from the defence-in-depth strategy to zero trust architecture, etc). To be consistent with the principle-based and technology-agnostic approach of the guidance, the Reserve Bank agrees to remove this specific recommendation from the guidance and focus on emphasising the protection approaches adopted by entities should be fit for purpose and be regularly updated.	B2.2 is revised as 'B2.2 The entity should regularly update its security controls to ensure the approaches it adopts remain commensurate to the entity's critical functions, cyber threat landscape and systemic importance'.
Part B: Capability Building_ B2. Protect	B2.3 There are potential challenges with providing ongoing support and maintenance in a legacy system environment. So B2.3 should be added with 'as appropriate'.	The intention of B2.3 is to help an entity properly manage its systems throughout its life cycle. An entity could decide not to update/maintain a legacy system if it believes doing so is not financially or operationally reasonable and choose to replace or decommission the legacy system. This is aligned with the recommendation of B2.3.2.	'as appropriate' is added to the end of B2.3.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part B: Capability Building_ B2. Protect	B2.3.2 Decommission and replacement of legacy systems could involve significant costs and resources. It is not necessary to replace legacy systems where other reasonable security measures designed to ensure a level of security appropriate to the risk are implemented. Regulated entities should be empowered to make risk-based decisions regarding their approach to legacy systems, which may include retaining them within the organisation for a period of time.	The non-binding nature of the guidance leaves the decision power in the hands of the regulated entities to decide on how they treat legacy systems. Legacy systems include end-of-life or unsupported software and devices. There are certain circumstances, as listed in B2.3.2, under which the entity should discontinue such systems. These circumstances include when no support is available, no patches are available to adequately address vulnerabilities, or no methods can be applied to segregate the system from other systems to mitigate the potential vulnerabilities, etc. The intention of the recommendation is to help regulated entities fully understand the risk associated with legacy systems. Plenty of evidence suggests that having legacy systems running has a wider impact on the cyber resilience of an entity as more vulnerabilities may be found and the impact and size of risk increases. CERT NZ provides a detailed explanation on how to deal with legacy systems.	No changes made.
Part B: Capability Building_ B2. Protect	B2.5: The reference to 'life cyber' should be to 'life cycle'	Typo.	B2.5 'life cyber' is amended to 'life cycle'.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part B: Capability Building_ B2. Protect	B2.6: Screening contractors and conducting background checks are too specific for principle-based guidance. If people have already been hired they do not need to be screened again as existing employees.	B2.6 is a high-level recommendation regarding identity and access management and the Reserve Bank does not agree that it is too specific for guidance. Existing employees that change roles to a sensitive position requiring privileged access to critical systems should be screened again to meet the entity's requirement of access management.	B2.6 is updated to reflect the pre-screening and access management for existing employees are needed if the employee changes roles.
Part B: Capability Building_ B2. Protect	B2.9 is too prescriptive. Using automated mechanisms to isolate affected information assets may not be appropriate in all circumstances. It may be costly to implement and may cause unnecessary disruption to business.	Automated mechanisms of isolating affected information assets in the case of an adverse event should only be used when an entity believes benefit outweighs the cost both financially and operationally.	B2.9 is revised as 'The entity could find it useful to implement automated mechanisms that can isolate affected information assets in the case of an adverse event as appropriate'.
Part B: Capability Building_ B3. Detect	B3.7.1 Should redraft this recommendation as 'security testing' rather than 'penetration testing' and make this as a baseline practice rather than an enhanced level of recommendation.	The Reserve Bank agrees that there is a wide spectrum of practices regarding security testing, from vulnerability assessments, scenario-based testing, penetration testing to more advanced approaches like red-team testing, etc. Entities should choose the appropriate testing method that is commensurate with their cyber risk profile and risk appetite.	In B3.7, B3.7.1 and B3.7.2, 'penetration tests' is revised as 'security tests' and the recommendations are revised to be baseline level rather than enhanced level.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part B: Capability Building_ B3. Detect	B3.7.2 In the case of red team testing, not all internal staff and departments critical to the cyber resilience of the entity need to be involved. Instead, only a minimal group of stakeholders will be informed to provide effective validation of the entity's alerting, monitoring and response capabilities.	This recommendation intends to ensure penetration testing is fully conducted and that the impact and gaps identified are understood by all relevant internal stakeholders and relevant third parties. The Reserve Bank acknowledges the special features of red team testing, which is not covered by the guidance since red team testing is regarded as an advanced level of practices. Regulated entities with capabilities to pursue a high level of cyber resilience are encouraged to use advanced methods, including red team testing, to test the effectiveness of their cyber resilience framework.	B3.7.2 is revised as 'The penetration tests should involve, **if deemed necessary**, all **relevant** internal…'
Part B: Capability Building_ B4. Respond and Recover	B4.1.3 Suggest adding that the severity and impact of a cyber-incident will dictate the level of stakeholder engagement.	Agree.	The following sentence is added to B4.1.3 'The level of stakeholder engagement should be informed by the severity and impact of a cyber incident'.
Part B: Capability Building_ B4. Respond and Recover	B4.3 Could be clarified that staff responding to a cyber incident or breach may outsource skills that are relevant to address the situation.	The Reserve Back acknowledges that some entities may outsource skills to deal with cyber incidents response and recovery. In that case, an entity should refer to Part D to ensure the third-party service providers have the capability to meet the requirements of the entity's cyber resilience.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part B: Capability Building_ B4. Respond and Recover	B4.7: Clarify the wording to read 'The entity should have processes and procedures in place to conduct a post-incident analysis to identify the root cause of its cybersecurity incidents, and integrate its findings back into its response and recovery plan'.	Agree.	B4.7 'ex post root cause analysis' is revised to 'a post-incident analysis to identify the root cause'.
Part B: Capability Building_ B4. Respond and Recover	B4.8 Need further clarification about common response and recovery plan to ensure developing and sharing plans for cyber incidents across the financial sector would not expose or increase the risk of further cyber incidents.	This recommendation aims to provide an advanced level of coordination among stakeholders of the financial system. Entities should always develop their own response and recover plan but should also take into considerations the actions needed from relevant stakeholders to better coordinate the response to cyber incidents. Entities should be able to decide what information is included in their 'common plan' to avoid being exposed to increased risk.	No changes made.
Part B: Capability Building_ B4. Respond and Recover	B4.8.1 Testing of common response and recovery plans with external stakeholder, especially network providers will improve the collective ability and speed to respond during a real-life incident. This recommendation should be of baseline level, not enhanced capability.	The benefit of joint testing is well acknowledged. Considering the diversified maturity of cyber resilience in different financial institutions, this recommendation will still be regarded as an enhanced level. To be more advanced and active in future (and strengthen cyber resilience), the Reserve Bank may develop the capability to coordinate joint testing of common response and recovery plans with the financial industry.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part C: Information Sharing Preamble	What's the expectation about sharing information other than the matters listed (indicators of compromise, cyber incidents, threats, vulnerabilities, risk mitigation, best practice and strategic analysis) in the preamble? 'Highly contagious' cyber threats is unsubstantiated and may unnecessarily fuel community concern and confusion.	The list of information that can be shared is only suggestive rather than exhaustive. 'Includes' does not limit the information that can be shared to the matters listed. It is well recognised by the industry that cyber threats are contagious. The contagion of cyber threats is also well documented by academia. To be neutral and avoid causing unnecessary confusion, the Reserve Bank agrees to remove 'highly' from the description of cyber threats.	'but is not limited to' is added in the second paragraph of the preamble of Part C. First sentence of the preamble of Part C is revised as 'Facing ever-evolving and ~~highly~~ contagious cyber threats…'
Part C: Information Sharing_C1. Channels and C2. Process	C1.3, C2.3 and C2.4 'could' should be replaced with 'would'.	C1.3, C2.3 and C2.4 are to recommend entities participate in information sharing groups. These practices are approved to be effective by industry experience.	In C1.3, C2.3 and C2.4, 'could' is replaced with 'would'.
Part D: Third-Party Management	Is Part D is intended to add an additional layer of third-party risk assessment besides BS11 Outsourcing Policy for large banks?	The Reserve Bank would like to emphasise that unlike BS11, the guidance on cyber resilience is non-binding and should not be read as an additional layer of any existing binding requirement by the Reserve Bank. As explained in the preamble of Part D, where an entity is required to comply with BS11, the guidance should be read in conjunction with BS11 because BS11 is not drafted specifically for managing outsourcing activities related to IT/cyber.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Part D: Third-Party Management Preamble	The preamble should keep a balance between the benefits and the risks associated with using third-party service providers. Prudent use of third-party services may reduce an entity's cyber risk, especially when the management of cyber risk is not within the core expertise of an entity.	The Reserve Bank acknowledges both the potential benefits and risks for entities using third-party service providers. As emphasised in the consultation paper, the Reserve Bank developed the guidance to be technology-agnostic and has no bias towards the use of any technology and innovation, including cloud computing services.	The following sentence is added in the preamble of Part D: 'If used prudently, third-party services may reduce an entity's cyber risk, especially for those entities that lack cyber expertise'. The second last paragraph is revised as 'If managed prudently, migrating to cloud may present a number of benefits... sufficient redundancy...' "However, using cloud services ~~does~~ brings ~~more~~ challenges to assess legal…"
Part D: Third-Party Management D3 Contract Negotiation	D3.1 Suggest softening the language to 'use best efforts' to negotiate because some large companies may be difficult to negotiate with. Suggest specifying which issues should be addressed in the contracts with cloud service	The intention of this recommendation is to suggest entities use contracts as an enforceable tool to manage their relationship with third-party service providers. The list of role and responsibilities of each party to be specified in the contracts are only suggestive rather than binding or exhaustive. Entities should decide what contents	D3.1 is revised as 'The entity should use contracts with third parties to capture cyber security considerations that are commensurate with the entity's cyber risk appetite. This may include roles and responsibilities of each involved party regarding data access, incident response and

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	providers to avoid hindering cloud service providers' ability to adopt new best practices or take advantage of technological advancements.	should be included in contracts to reflect their risk appetite and the features of the outsourced activities/services.	communication, business continuity plan, termination, and data portability, etcetera'.
Part D: Third-Party Management D4. Ongoing Cyber Risk	Suggest including relevant contents of D4 in Part B (Capability building) to assist entities so that they can understand how to build capabilities in respect of third-party management.	Managing cyber risk associated with using third-party service providers on an ongoing basis after signing the contract relates to each stage of capability building for an entity: Identify, Protect, Detect, Respond and Recover. The purpose of including relevant contents in Part D rather than imbedding them in Part B is to raise special attention to the importance and challenges of managing cyber risk associated with using third-party service providers.	No changes made.
Part D: Third-Party Management D4. Ongoing Cyber Risk	D4.1.1 Intent of the principle would be clearer if it was amended to read 'Clearly identify and document the cyber risk associated with **using** third party **service providers** and update this information on a regular basis'.	Agree.	D.4.1.1 revise to read 'Clearly identify and document the cyber risk associated with **using** third-party **service providers** and update this information on a regular basis'.
Part D: Third-Party	D4.1.2: Ask the intention of this requirement. Are banks expected to	D4.1.2 sets out recommendations for entities to consider any intrusions from third-party connections when developing cyber	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
Management D4. Ongoing Cyber Risk	have proactive capabilities to monitor third party connections into their networks, or is it sufficient that they rely on the end-point security controls they already have within their organisation?	capabilities to detect and prevent. Entities should decide whether to rely on their existing end-point security controls within their organisations or if they should build proactive capabilities for monitoring third-party connections into their network according to the entities' cyber risk appetite.	
Part D: Third-Party Management D4. Ongoing Cyber Risk	D4.1.3: It is not a common market practice for a bank to be "tracking actively" third party employee access. Suggest moving this recommendation as an enhanced rather than a baseline level.	Entities need to have management solutions to control access to third-party service providers in a secure way to avoid any compromises. The Reserve Bank believes it is appropriate to keep D4.1.3 as a baseline level recommendation.	No changes made.
Part D: Third-Party Management D4. Ongoing Cyber Risk	D4.1.4: Involving third-party service providers in response testing is not always practical due to the cost, effort and time required. Recommend it be risk-based and include third parties that are part of the core response capabilities for incident scenarios. Involving third parties in response testing should be an enhanced level of recommendation, because financial entities will not always be able to contractually agree such participation with their third party	The Reserve Bank acknowledges that conducting response testing with third-party service providers needs substantial efforts and resources. Therefore, D4.1.4 only recommends doing so with critical service providers that provide critical functions for an entity. The Reserve Bank agrees with making this recommendation as an enhanced level. If financial institutions choose to rely on the assurance from their third-party service providers that the service providers conduct response testing regularly and review the response plan regularly, it should not affect the financial institutions' understanding of their own	D4.1.4 is revised by removing 'and involve them in response testing'. One additional recommendation is added as D4.3 as an advanced level of recommendation 'The entity could find it useful to conduct response and recovery testing with its third-party service providers and use the testing results to improve its response and recovery plans'.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	service providers, or it may only be agreed on the basis of a significant fee. It will be sufficient for financial entities to make sure that third party service providers of their critical functions have adequate response plans that are tested regularly.	responsibilities, nor should it affect the financial institutions' capability of taking actions to coordinate with their third-party service providers in incident response.	
Part D: Third-Party Management D4. Ongoing Cyber Risk	D4.2: Ask for definition or guidance of an 'entity's critical functions'. Unclear about how banks should prepare for transitioning to alternative service providers, and it may not be possible for certain critical services to be performed in-house.	The definition of 'critical functions' is already provided in the Glossary. We agree that not all functions need to be prepared to move to alternative channels. The entity should be able to determine to what extent it prepares to move services to alternative channels, according to the criticality of the services for the entity's operation and the risk appetite of the entity.	D4.2 is revised as 'The entity should assess…, and include transitioning to alternative service providers or performing critical services in-house in its business continuity plan that is commensurate with the criticality of the services and the entity's risk appetite'.
Part D: Third-Party Management D5. Review and Accountability	D5.1: The wording 'at least through the providers' self-assessment if not through conducting its own assessment' may cause confusion.	An entity should decide how to assess its third-party service provider's cyber security capability according to the entity's risk appetite and capability. The assessment can be achieved through services providers' self-assessment, certification,	D5.1: Delete 'at least through the providers' self-assessment if not through conducting its own assessment,' but add 'The assessment can be

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	Suggest defining 'regularly'.	external audits, or conducting their own assessment by the entity. The entity should decide the frequency of assessing their third-party service providers' cyber security capability according to its risk appetite. The Reserve Bank does not intend to put a frequency in the non-binding guidance.	achieved through services providers' self-assessment, the entity's own assessment, or assessment by independent third parties'.
Part D: Third-Party Management D6. Documentation	D6.1: Clarify what is meant by 'interconnection with other entities'. Is this referring to APIs, interconnectedness in the context of reliance, or something else?	'Interconnection with other entities' may mean different things for different types of entities and the different services they provide. For example, payment or settlement systems should consider their interconnections with their participants, and banks acting as direct participants for those indirect participants in payment/settlement systems should also consider their interconnections with other banks. Development in Fintech brings entities more possibilities of having interconnection with non-financial institutions. Interconnection is a broad concept and D6.1 does not intend to provide an exhaustive list.	No changes made.
Part D: Third-Party Management D7. Termination	D7.1: The termination/exit of using third party service providers is ordinarily contractually provided for, including transition and service continuation provisions. Need clarification about the expectation of the regulator.	Establishing a termination/exit strategy does not only mean including specific terms in contracts with third-party service providers. It also includes comprehensive internal preparation/review and actions around how to execute. The guidance is non-binding and does not put additional requirements to BS11 Outsourcing Policy.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	Clarify whether D7.1 puts requirements to report to the regulator in addition to BS11.		
Part D: Third-Party Management D8. Outsourcing to Cloud Service Providers	D8: Will banks be required to obtain formal approval from RBNZ for usage of cloud-based services or just provide notification? What is RBNZ's intention around and what will RBNZ do with the information?	It is not a binding requirement to obtain formal approval from the Reserve Bank when adopting cloud computing. However, we do recommend entities to notify the Reserve Bank as early as possible when considering adopting cloud computing.	No changes made.
	Clarify whether D8 requires an entity to notify the regulator in addition to BS11.	Currently, the Reserve Bank puts no prescriptive requirements on using cloud computing. The main purpose of being notified is to monitor systemic risk and explore the necessity of developing policies in this area in future. Large banks that are required to comply with BS11 Outsourcing Policy should not read D8 as an additional requirement to notify the Reserve Bank.	
	Should specify which functions the Reserve Bank would consider to be critical.	As explained for D4, the definition of 'critical functions' is provided in the Glossary. An entity should decide which functions are critical to their operation.	
	Should specify what decision-making process refers to since entities may, or may not, run a full	Internal decision-making processes differ from one entity to another. Generally, the Reserve Bank expects to be informed	

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	procurement process before selecting a cloud service provider.	by an entity before it finalises the agreement with its cloud service provider.	
Part D: Third-Party Management D8. Outsourcing to Cloud Service Providers	D8.3 The location of data in transit and data in use (processed) should not be equated with the location of stored data. Data in transit and data in use in cloud computing is generally ephemeral and encrypted so does not create the same data location and sovereignty issues as stored data or data at rest.	The Reserve Bank acknowledges that encryption is an effective method to mitigate risk. However, it does not mean encryption can eliminate jurisdiction risk associated with data in transit or data in use. Financial entities should be fully aware of the jurisdiction risk that the entity's data 'in cloud' is exposed to. An entity's awareness of the jurisdiction risk and the ability to assess the jurisdiction risk associated with using cloud computing services should not be limited to stored data or data at rest but also should include data in transit and data in use. The Reserve Bank agrees to amend the wording to emphasise the jurisdiction risks rather than the specific location of data.	D8.3 is revised as 'D8.3 The entity should be aware of the jurisdiction risk associated with data stored, processed and transmitted in cloud, including data replicated for provision of backup or availability services. The entity should assess the potential legal risk, compliance issues and oversight limitations associated with outsourcing to cloud service providers'.
Part D: Third-Party Management D8. Outsourcing to Cloud Service Providers	Ask for exemption for outsourcing to public cloud service providers regarding B1.3 (mapping network resources), B1.4.1 (testing before introducing new features), B3.7 (security testing), B4.7 (root cause analysis), and B4.8.1 (joint test response and recovery plan).	The principle of proportionality applies to the guidance, which means entities can decide the extent to which the recommendations in the guidance are relevant to their practices. The Reserve Bank acknowledges the features of public cloud computing services and makes the relevant recommendation in D8.4 that 'the entity should carefully consider different levels of responsibilities when entering into an agreement with its cloud service provider'.	No changes made.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
		The responsibilities include all aspects mentioned in Part A, B and C of this guidance. Entities can choose from a wide spectrum of practices by either conducting their own testing and root cause analysis, for example, or rely on the testing and root cause analysis provided by their cloud service providers, as long as doing this will not affect the entities' understanding of its own responsibilities and taking actions to coordinate with their cloud service providers. The Reserve Bank does not believe it is necessary to make exemptions for outsourcing to cloud computing service providers in any recommendations regard capability building in Part B.	
Part D: Third-Party Management D8. Outsourcing to Cloud Service Providers	Substitutability and being able to move data/services between providers is relevant to outsourcing activities, rather than being unique to cloud computing services. D8.6 should be integrated into D4.2 to reflect portability and interoperability as a general issue relevant to different types of infrastructure and services, rather	We acknowledge the importance for entities evaluating and considering the substitutability of their service providers and portability and interoperability if the services are related to storing and/or processing data. The recommendation is intended to be technology-agnostic. D4.2 is about on-going risk management and business continuity plans. Consideration of service portability and interoperability in outsourcing contract negotiation belongs to the contents of D3.	D8.6 is deleted, and the following contents are added to D3.3 as an enhanced level recommendation for contract negotiation: 'The entity may find it helpful to consider portability and interoperability of their data and applications and include provisions in its outsourcing contracts to avoid vendor lock-in'.

Comments	Summary of responses received	RBNZ analysis	Amendments to the proposals
	than unique to cloud computing service.		
Guidance—Appendix	Suggest regularly updating the Glossary to reflect the change in the cyber landscape and innovation. Ask whether the glossary will only be updated to coincide with the review of the Cyber Lexicon.	Although the Glossary of the Reserve Bank guidance has been developed by keeping aligned with FSB's Cyber Lexicon and the glossary used by NIST Computer Security Resource Centre, updates of the Glossary are not limited to or associated with the aforementioned documents. We will regularly review the guidance (including the Glossary) as appropriate to make sure it is fit for purpose. However, new terms associated with innovation in information technology or cyber risk management that are not covered by the Reserve Bank guidance are out of the scope of the Glossary.	No change made.
Guidance—Appendix	Suggest adding Financial Services Sector Cybersecurity Profile (FSSCP) to the recommended frameworks that regulated entities can refer to.	We acknowledge that Financial Services Sector Cybersecurity Profile is a useful tool for mapping risk profiles and is consistent with the NIST Cybersecurity Framework and other major international standards regarding cybersecurity. It is also aligned with the draft guidance prepared by the Reserve Bank. In November 2020, the FSSCP has been updated and renamed as Cyber Risk Institute Cybersecurity Profile.	Cyber Risk Institute Cybersecurity Profile is added in the list of recommended frameworks in the Appendix to the Guidance.