Reserve Bank of New Zealand
Te Pūtea Matua

# Cyber Resilience Data Collection Proposals

8 May 2023

CONSULTATION PAPER

# Non-technical summary

Cyber risk – both malicious and non-malicious – continues to grow as an area of focus within the financial sector. Cyber risk can impact financial stability through loss of confidence, and lack of substitutability and interconnectedness. Building and maintaining cyber resilience is important for promoting a sound and dynamic financial system.

The Reserve Bank of New Zealand – Te Pūtea Matua (the Reserve Bank) has been undertaking a three step approach to supporting building cyber resilience in our regulated entities. The steps are as below:

- Step 1: Cyber Risk Management Guidance (Published Q2 2021);
- Step 2: Cyber Data Collection Requirements and Information Sharing Arrangements (the proposals in this paper relate to this step); and
- Step 3: Enhanced Coordination and Response to Cyber Incidents (New Zealand-based decisions taken in Q2 2022, and trans-Tasman decisions taken in Q4 2022).

We propose two key components to improve our collection of cyber related information:

- *Cyber incident reporting:* a requirement to report all material cyber-incidents to the Reserve Bank as soon as practicable, but within 72 hours, (see Annex A for the reporting template) and to report all cyber incidents (material and non-material) on a periodic basis); and
- *Cyber capability survey:* a periodic cyber resilience survey about organisation capabilities (see Annex B for the draft questionnaire).

Collecting this information will support a number of important functions:

- measuring the effectiveness of our cyber resilience policy settings and inform further policy developments;
- helping guide meaningful discussion between financial regulators and regulated entities;
- supporting financial system risk monitoring efforts; and
- providing insights and intelligence on the cyber threat landscape that could be shared with industry, public sector agencies or others.

We have worked closely with the Financial Markets Authority - Te Mana Tātai Hokohoko (FMA) on these proposals reflecting our shared interest in cyber resilience in the financial sector arising from New Zealand's 'twin peaks' approach to prudential and conduct regulation. Our proposal is that the material incident reporting template can be used for reporting material cyber incidents to both the Reserve Bank and the FMA. We propose to share information collected under the two periodic surveys with the FMA and other relevant agencies. Our intention is to improve information flows between financial regulators and reduce compliance costs for our regulated entities by reducing the number of requests for cyber related information.

## What do you think?

Please refer to the consultation questions set out in Section 8.1 of this consultation paper.

All responses should be emailed to cyberresilience@rbnz.govt.nz or sent to:

Cyber data collection consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

We welcome submissions until 5pm, 3 July 2023.

# Contents

# 1 Introduction

The ability of cyber attackers to undermine, disrupt, and disable information and communication technology systems used by financial entities is a threat to financial stability and one that requires additional attention. Cyber risk can impact financial stability through loss of confidence and lack of substitutability and interconnectedness. Attackers have broad access to technology, allowing them to operate across borders and to attack financial entities either for profit or simply to disrupt. The COVID-19 pandemic has only heightened awareness of the vital importance of protecting digital systems and connectivity to ensure the continuity of economic and financial activity. Malicious cyber incidents are not the only risk – non-malicious internally driven cyber incidents remain a risk for financial entities.

The Reserve Bank is the prudential regulator of banks, insurers, non-bank deposit takers and financial market infrastructures. The Reserve Bank's role as prudential regulator includes promoting the safety and soundness of our regulated entities as a part of our financial stability mandate. The growing cyber risks facing the financial sector mean that we seek to promote cyber resilience in our regulated entities.

We observe that—with some notable exceptions—most successful cyber attacks impacting the financial sector affect one institution and produce limited damage. However, a successful attack with enough technical force to disable or disrupt a key institution or spread through the financial system could become a systemic event. A significant system failure could have the same effect. Key impact channels could include the following:

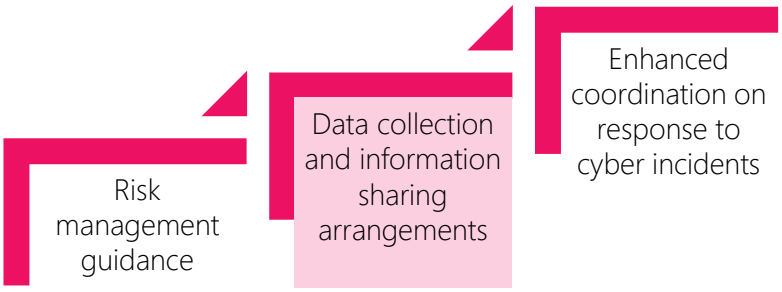
- Lengthy outages and compromised data integrity can lead to a loss of confidence in an institution or the wider financial system. Liquidity is likely to be affected quickly if confidence is lost.
- The loss of a key service — without easy substitution by other service providers — is another channel through which cyberattacks can affect financial stability.
- Weaknesses in technology used across the industry can expose many institutions to threats simultaneously and have a broad effect on the entire financial sector. Interconnectedness—within the financial system and across technologies—also increases the financial stability risk arising from cyberattacks.

Building and maintaining cyber resilience is ultimately a shared responsibility. The nature of cyber risks means that a collective effort is needed to build effective defences and address weak points that might be easily exploited. Domestically, cyber resilience involves various public sector agencies, the private sector and the general public. Internationally, it is necessary to cooperate across jurisdictions because cyber risks can spread beyond borders. Information on cyber threats and organisational capabilities to protect, detect, respond and recover from cyber incidents plays a vital role in facilitating a joined up and collective response to growing cyber risks.

In April 2021 we published *Guidance on Cyber Resilience*[1] for our regulated entities (the Guidance). The Guidance sets our expectations (as the prudential regulator) on how our regulated entities can build cyber resilience to help promote a sound and dynamic financial system.

[1] Guidance on Cyber Resilience, Reserve Bank of New Zealand (April 2021)

The Guidance was the first element of our three step approach towards building cyber resilience and is relevant to all Reserve Bank regulated entities (including banks, non-bank deposit takers, insurers and financial market infrastructures (FMIs)). Subsequent steps involve developing a **cyber data collection**, establishing **information sharing arrangements**, and building **enhanced incident response coordination** protocols among public and private sector bodies.




This consultation paper presents our proposal to establish a cyber data collection for banks, non-bank deposit takers and insurers (referred to in this paper as Reserve Bank regulated entities). Notification requirements (including material cyber incidents) for FMIs are contained separately in our proposed standards for FMIs.2 The purpose of the cyber data collection is to:

- enable monitoring of and reporting on cyber risks;
- support risk management guidance and practices by establishing industry benchmarks;
- support incident response practices; and
- refine cyber risk policy settings.

You are invited to make a submission on any of the issues covered in this paper. Further feedback will help us to refine our approach to collect data and share information about cyber resilience.

## 1.1 Working with the Financial Markets Authority

The Reserve Bank works closely with the FMA to improve our coordination on cyber resilience policy relating to our respective regulated entities. The nature of New Zealand's 'twin peaks' approach to prudential and conduct regulation means that we have shared interests in the cyber resilience of the financial sector. Reflecting these shared interests we are closely working with the FMA on the proposals contained in this document, including proposing to use a common reporting template and to share cyber information collected in order to minimise the compliance burden for entities that are regulated by both the Reserve Bank and the FMA. The information proposed to be collected reflects our respective interests in the cyber resilience of our regulated entities.

In 2022 the Reserve Bank progressed, with other financial regulators, in particular the FMA, actions to improve our coordination in responding to cyber incidents. Domestically, within the Council of Financial Regulators (CoFR), we agreed to a Cyber-Attack Response Protocol detailing how financial regulators will work together in responding to a cyber-attack impacting on a regulated entity. We have also worked with the Australian Council of Financial Regulators to agree to a trans-

[2] Our proposed standards for FMIs were consulted on in 2022. Standard 23B provides for notification requirements for FMIs for material incidents.

Tasman Playbook for how financial regulators in Australia and New Zealand will work together in the event of an incident impacting an entity regulated in both countries.

## 1.2 Feedback from consultation on cyber resilience guidance

In October 2020, we presented our initial views about gathering and sharing cybersecurity related information in our consultation paper on cyber resilience guidance. Key feedback from submitters included:

- Widespread support for our intention to establish a cyber-resilience information collection;
- The need to take a coordinated approach to collecting information to minimise compliance costs and avoid duplication;
- The need for information to be transmitted and stored securely; and
- Cyber related information is often highly sensitive and any information that is shared outside the Reserve Bank should be anonymised.

As noted in our responses to these submissions, we see merit in these key points of feedback and they will shape our cyber data collection and information sharing protocols.

# 2 Overview of Cyber Data Collection Plan

A cyber incident (as defined in paragraph 0) that affects the security, or the ability to provide services, of a Reserve Bank regulated entity can have significant implications for the soundness of an individual entity as well as the wider financial system. As a prudential regulator, it is important that we are able to adequately understand the nature of cyber risks facing our regulated entities as well as their resilience in being able to respond to cyber incidents.

In many jurisdictions, it is mandatory for financial entities to report cyber incidents to prudential regulators. This improves the ability of prudential regulators to understand and respond to cyber threats. Incident reporting frameworks adopted in different countries range from formal communication (following a pre-set template) to informal communication. Incident reporting also typically involves the requirement to report within a specified time frame and a pre-defined threshold that triggers reporting on a 'significant' or 'material' cyber incident. There is also typically a requirement to report non-material incidents within a less urgent time frame such as quarterly or semi-annually.

We propose two key components for our collecting cyber related data:

- Cyber incident reporting: a requirement to report all material cyber-incidents to the Reserve Bank as soon as practicable, but within 72 hours, (see Annex A for the reporting template) and to report all cyber incidents (material and non-material) on a periodic basis); and
- Cyber capability survey: a periodic cyber resilience survey about organisation capabilities (see Annex B for the draft questionnaire).

The cyber incident reporting requirement will help fill two gaps. First, it will contribute to a more coordinated response by the RBNZ and other government agencies to cyber-attacks when they do occur. Second, it will improve our understanding of the scale and severity of cyber risk in the financial sector.

The periodic survey is focused on gathering information about organisational capabilities to build and maintain cyber resilience. Broadly, the topics covered in the periodic survey will mirror those addressed in the Guidance. The survey will improve our understanding of the ability of regulated entities to manage their cyber resilience and the overall level of cyber risk in the financial sector.

Combined, we envision that these two cyber data collection proposals will support a number of important functions, including:

- measuring the effectiveness of our cyber resilience policy settings and inform further policy developments;
- helping guide meaningful discussion between financial regulators and regulated entities;
- supporting financial system risk monitoring efforts; and
- providing insights and intelligence on the cyber threat landscape that could be shared with industry, public sector agencies or others.

In our previous consultation on the cyber risk management guidance (in late 2020), all submitters supported mandatory reporting of material cyber incidents with a clearly defined threshold of materiality. For the reporting timeframe and information requirements, we aim to strike a balance so that we are adequately informed about a cyber incident in a timely manner and regulated entities will still have sufficient time to evaluate the impact of an incident and focus on their response efforts. We also consider that all cyber incidents, regardless of severity, should be reported on a less urgent time but regular time frame.

We have worked with the FMA to develop alignment for entities that are regulated by both the Reserve Bank and the FMA. Our proposal is that the reporting template for material cyber incidents can be used for satisfying reporting requirements for both the Reserve Bank and the FMA. This is intended to avoid duplication of collection of similar information between financial regulators. We also propose that information gathered from the two proposed periodic surveys will be shared with the FMA.

# 3 Cyber incident reporting

In order to better understand the nature of cyber incidents impacting our regulated entities and to understand specific events impacting individual entities, we are proposing the collection of two types of data relating to cyber incidents.

- First, we propose mandatory reporting of all material cyber incidents (as defined in paragraph 0) to the Reserve Bank as soon as practicable, but no later than 72 hours after detection (see paragraph 0 for further detail).
- Second, we propose that entities report all cyber incidents, regardless of materiality, to the Reserve Bank on a six-monthly basis for large entities and annually for all other entities.

We note that in referring to 'cyber incidents' we use the definitions contained in the glossary of our Guidance on Cyber Resilience (which draws on the 'cyber lexicon' developed by the Financial Stability Board). This definition of a cyber incident is:

> *A cyber event that:*
>
> *i jeopardises the cybersecurity of an information system or the information the system processes, stores or transmits; or*
>
> *ii violates the security policies, security procedures or acceptable use policies;*
>
> *whether resulting from malicious activity or not.*

## 3.1 Mandatory reporting of material cyber incidents

There are three key elements to our proposal for mandatory reporting of all material cyber incidents: the reporting timeframe, what constitutes a material incident, and what information is required to be reported. Each of these elements is discussed below.

### Timeframe for mandatory reporting of material cyber incidents

Our proposed approach is that all material incidents (as defined below) must be reported as soon as practicable after they are detected but no later than 72 hours. Different jurisdictions use a range of timeframes for incident reporting. Our proposed approach is similar to that required in Australia. It seeks to accommodate a wide range of entities and the diverse nature of cyber incidents.

While our proposed timeframe provides for notification of incidents no later than 72 hours after detection of a material incident to accommodate a range of scenarios, our expectation is that entities will report the incident to the Reserve Bank as soon as practicable. We recognise that cyber incidents evolve and the nature of the information available will also evolve over time. We also recognise that initial reporting may be of incomplete information – we consider it preferable that an incident is reported with incomplete information which is later updated, rather than holding off to ascertain more information about the nature of the incident.

The FMA will also impose this same reporting timeframe under the standard condition for business continuity and technology systems that will apply to financial institutions[3] licences under the new Conduct of Financial Institutions regime.[4] Alignment on reporting timeframes will ensure consistency for entities that are regulated by both the Reserve Bank and the FMA. We note that the FMA has different reporting requirements for financial advice services than those that will apply to financial institutions.[5]

Timely incident reporting will support the Reserve Bank's supervisory engagement with entities as well as enabling the Reserve Bank to work with other Council of Financial Regulator (COFR) agencies to respond to a cyber incident as appropriate.

**Q1** Do you have comments on our proposed cyber incident reporting timeframe?

## Materiality threshold definition and guidance

### Definition

Our proposed approach requires that all material cyber incidents are reported to the Reserve Bank. We propose the following definition of what constitutes a material incident:

> *A material cyber incident is one which materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of its stakeholders such as depositors, policyholders, beneficiaries, other customers, system participants, or more broadly raises prudential concerns.*

This definition is based off APRA's materiality definition, adapted to be appropriate for all RBNZ regulated entities.

We considered definitions from both APRA and the FMA on what constitutes a material cyber incident to inform our proposed definition:

- The FMA's does not use the term 'material cyber incident' in its standard condition for financial institutions. However, the standard condition requires notification of an "event that materially impacts the operational resilience of your critical technology systems".[6]
- APRA defines a material cyber incident as one which materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.

The FMA's definition of materiality appears to be somewhat narrower than the APRA definition due to its focus on 'operational resilience' and 'critical technology systems'. The APRA definition could capture these elements through the use of the term 'cyber incident' which we define and use in our *Guidance on Cyber Resilience* but also appears to be slightly broader due to the focus on outcomes for depositors, policyholders, beneficiaries or other customers. Despite this, in

[3] 'Financial institution is a defined term under the Financial Markets (Conduct of Institutions) Amendment Act 2022.
[4] Standard-conditions-for-financial-institutions.pdf (fma.govt.nz)
[5] Standard-Conditions-for-full-FAP-licences.pdf (fma.govt.nz)
[6] Critical technology" is defined as that which supports any activity, function, process, or service, the loss of which would materially affect the continued provision of the financial institution service or ability to meet the licensee obligations. "Operational resilience" is defined as 'the preservation of confidentiality, integrity and availability of information and/or technology systems.' The explanatory notes to the standard condition clarify that notification must be made of "any technological or cyber security event that materially disrupts or affects the provision of the financial institution service, or has a material adverse impact on consumers". The explanatory notes state that a minor event such as receiving a 'phishing' email that is not successful would not be material in this context.

practice we consider that there is unlikely to be substantive differences in the types of incidents reported.

On balance, we consider that there is value in closer alignment to the APRA definition given our aligned focus on prudential concerns and the number of our regulated entities that have close ties to Australia. This approach would also make it simpler for these entities to align their reporting practices.

The Reserve Bank currently requires material breaches of key bank prudential requirements to be reported to the bank within reasonable timeframe although this does not currently apply to cyber incidents. However, the framework to identify material breaches of conditions has some useful guidance that we think is relevant for identifying material cyber incidents. This is discussed in more detail further below.

For clarity, the proposed materiality definition is only to apply to the Reserve Bank's material incident report requirement. The FMA's incident reporting requirement remains a separate requirement as outlined in their standard condition for business continuity and technology systems that will apply to financial institutions licences.

**Guidance**

To help reporting entities consider how a cyber incident could present material impacts and raise prudential concerns, we have adapted some guidance from the Reserve Bank's framework for breach reporting for registered banks. In assessing materiality, we consider that the following elements should be taken into account:

- The impact of the cyber-incident on the entity's ability to carry on business in a prudent manner;
- The extent to which the cyber-incident could result in financial consequences to the New Zealand financial system or to other financial entities;
- The extent to which the cyber-incident had/has a negative impact on stakeholders such as customers, investors or system participants;
- The extent to which the cyber-incident could have a significant adverse impact on the entity's reputation;
- How long the cyber-incident lasted (if already remedied), or is expected to continue;
- Whether the cyber-incident is an isolated incident, or part of a recurring pattern of cyber-incidents;
- The extent to which the cyber-incident indicates that the entity's internal control frameworks to ensure compliance with the conditions of registration are inadequate; and
- The nature of the underlying cyber-incident.

**Q2** Do you have comments on our proposed definition of materiality?

### Reporting template for cyber incidents

We recognise the importance of streamlining cyber incident reporting requirements and are working with the community of relevant agencies to make this reporting as efficient as possible. However, crafting a single cyber reporting requirement that is suitable for all relevant agencies is not likely to be feasible given that these agencies have their own mandates and areas of focus. For example, the privacy breach reporting requirement for the Office of the Privacy Commissioner (OPC) focuses on potential harms caused by privacy breaches, which has only limited overlap with the broader concept of cyber incident reporting than the Reserve Bank's focus on financial stability requires. However, we think it is feasible to align reporting requirements for financial regulators. For entities that are regulated by both the Reserve Bank and the FMA, we intend that our proposed incident notification template can be used for reporting to both regulators to avoid duplication.

After considering a range of existing reporting templates, we have adapted the approach taken by the Monetary Authority of Singapore. Its cyber incident reporting template includes three main elements and contains a mix of qualitative and quantitative information. The first element is information about the cyber incident after it is first detected. The second element is a flow of information about the incident as it is unfolding and response measures are deployed. The third element is a post incident report comprising the first two elements together. We consider that these three elements are necessary for the Reserve Bank to play its role in a coordinated response effort and feed into broader risk monitoring and information sharing efforts on understanding the cyber resilience of the New Zealand financial sector and its potential impacts on financial stability.

The draft cyber incident reporting template is provided in Annex A.

| | |
|---|---|
| **Q3** | Do you have comments on our proposed cyber incident reporting template? |

## 3.2 Periodic reporting of all cyber incidents

In addition to immediate reporting of material incidents, we are proposing to collect periodic information on all cyber incidents that have occurred. This would capture and collate both incidents already reported as material as well as less serious cyber incidents. We are still to develop a standardised approach to collection of this data, but envision collecting data on the number of cyber incidents, type of cyber incident (e.g. malware or DDOS) and the impact of the incident (e.g. IT outage or theft/loss of information). This would encapsulate the key information about an incident contained in our proposed template for material incidents. We propose that this information is reported on a six-monthly basis for large entities (as defined below) and annually for all other entities.

| | |
|---|---|
| **Q4** | Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting? |

## 3.3 How will we use the cyber incident reporting information we collect?

As outlined in section 1.1, CoFR has agreed to a cyber-attack response protocol for detailing how financial regulators will work together in responding to a cyber-attack impacting on a regulated entity. The purpose of this protocol is to facilitate a co-ordinated response to communication and collaboration across New Zealand Council of Financial Regulators (CoFR) agencies. We, and other

financial regulators, cannot provide a technical response and we do not seek to get in the way of incident resolution by an entity.

We will use the information gathered through cyber incident reporting to support any necessary regulatory response and to ensure that there is co-ordinated communication and engagement from financial regulators. Our proposal will ensure that details of cyber threats are communicated in near real time to improve situational awareness, prevent attacks spreading and preserve confidence in the economy.

Periodic cyber reporting will round out our understanding of cyber risk impacting the financial sector beyond material incidents. Better understanding of cyber risks facing the financial sector will support informing our policy and supervisory approach to cyber resilience. Collecting this information will allow the Reserve Bank to better understand and assess the nature of cyber risk impacting the New Zealand financial sector.

# 4 Cyber Resilience Survey

As well as better understanding of the nature of the cyber threats facing our regulated entities and the New Zealand financial sector, we want to better understand the cyber resilience capabilities of our regulated entities. For this reason we are proposing to establish a periodic survey of regulated entities on their cyber resilience capabilities.

Periodic surveys are a common tool for financial sector regulators to measure and monitor cyber resilience capabilities among their regulated entities.[7] The content and format of these periodic surveys vary considerably across jurisdictions and this largely reflects differences in domestic policy settings.

While there are a differences of approach to collating such information across jurisdictions, well-recognised and established cybersecurity frameworks, such as those from the National Institute of Standards and Technology (NIST) and the International Organisation for Standards (ISO), are used to judge cyber resilience and form a basis for common understanding. The Reserve Bank's cyber resilience guidance also utilises these frameworks. Our proposed capability survey is based on our guidance document. We consider that this approach will assist entities in reporting given the link to our guidance as well as supporting, where appropriate, information sharing domestically and with other jurisdictions.

## 4.1 Structure of the periodic survey

We propose that the periodic survey for regulated entities should be structured around the four chapters of the Guidance (i.e. governance, capability building, information sharing, and third party management).

The Guidance is presented as a set of best practice recommendations for building cyber resilience and this does not readily lend itself to measurement in a way that is directly suitable for a periodic data collection. We have therefore addressed this in our survey questions in two ways:

- First, at a reasonably granular level but not for each and every recommendation, reporting entities are asked to indicate the degree to which they are following the Guidance. While this approach is self-assessed, it aims to balance getting a meaningful benchmark of how the Guidance is being taken up by industry and minimising the reporting burden. Candid assessments of current capability will enable entities to think about their current performance as well as contributing to understanding their relative performance compared to the wider sector.
- Second, we have crafted a series of quantitative questions that are closely related to various aspects of the guidance. These quantitative questions are intended to help provide some concrete measures of cyber capabilities among reporting entities and includes a focus on the resources that entities allocate to cyber resilience (i.e. staff count and financial inputs).

[7] Australia, the U.K., Singapore and Hong Kong are just a few examples of jurisdictions where financial sector regulators have established periodic cyber data collections. In New Zealand, the Financial Markets Authority conducted a survey on cyber resilience capabilities of a sample of its regulated entities and published the results in a 2019 report: https://www.fma.govt.nz/assets/Guidance/Cyber-resilience-in-FMA-regulated-financial-services.pdf.

A draft survey questionnaire is provided in Annex B.

| | |
|---|---|
| **Q5** | Do you have comments on our proposed periodic cyber resilience capability survey? |

## 4.2 Frequency of reporting for the periodic survey

We consider that information on cyber capabilities should be collected regularly but not too frequently. A very frequent survey would provide more up to date information as cyber threats evolve but this needs to be balanced against the costs of collecting the data. Collecting information too infrequently would create an undesirable gap in our understating of cyber risks in a quickly evolving environment.

For the reasons noted in the previous paragraph, we consider that an annual or biennial (every two years) survey on cyber capabilities would be appropriate. Smaller scale institutions would, generally speaking, be more resource constrained and pose less risk to the financial system so it seems reasonable to collect cyber capability data less frequently than for larger or systemically important institutions. We believe that large institutions should be required to complete cyber capability surveys annually and all other institutions should do so every two years. We propose that 'large' for the purpose of this cyber data collection is assets in excess of $2 billion NZD.

We welcome your feedback on the proposed frequency of the cyber capabilities survey and the definition of a large reporting entity.

| | |
|---|---|
| **Q6** | Do you have comments on our proposed frequency of reporting or the threshold for reporting more frequently? |

## 4.3 How will we use this information?

Collecting information on the cyber resilience of entities will improve our understanding of the resilience of the finance sector at both an individual and sector wide level. More specifically, it will inform our supervisory engagement with individual entities on their cyber resilience and more broadly it will assist in informing our overall policy approach for cyber resilience. We will also explore how to best publish trends, key lessons or insights – on an aggregated or anonymised basis – to inform broader understanding of cyber resilience in the financial sector.

# 5 Information sharing and working with other agencies

## 5.1 Safeguarding the information we collect and share

We recognise that cyber related information can be highly sensitive and are firmly committed to ensuring that appropriate controls are applied to the storage, sharing and publication of all cyber information collected by the Reserve Bank from its regulated entities. We will be utilising our existing information sharing arrangements with the FMA to share information collected under these proposals, including where appropriate entity specific information. These arrangements will ensure that information is protected in the appropriate manner. Where information may need to be shared with other agencies, such as the NCSC, we will ensure appropriate protections are put in place.

Certain information that we are proposing to collect is intended to be shared with various forums, including public sector agencies with an interest in cyber resilience and industry itself. In these instances, we would only share information after considering the need to protect privacy and commercially sensitive elements of the information. Any broader publication of cyber related information would be aggregated or anonymised.

## 5.2 Working with the Financial Markets Authority

The Reserve Bank and the FMA have shared interests in the cyber resilience of our regulated entities through our roles as the prudential and conduct regulators respectively within New Zealand's financial system. As members of COFR we work closely together on our cyber policy to ensure alignment where appropriate and to minimise compliance costs associated with our requirements.

In November 2022, the FMA confirmed that the standard conditions that will apply to financial institution licences under the new conduct of financial institutions regulatory regime. The FMA will impose the same notification timeframe requirement for material incidents for financial institutions as we have proposed in this consultation paper for our regulated entities.[8]

For entities that are regulated by both the Reserve Bank and the FMA, we intend that our proposed incident notification template can be used for reporting to both regulators to avoid duplication. For example, if notification is required by both the FMA's standard condition for financial institutions and the RBNZ requirement, entities can send the same completed template to both the RBNZ and FMA. We also propose to share information collected under the two periodic reporting proposals. Information will be shared consistent with our statutory functions and our memorandum of understanding.

As members of COFR, the Reserve Bank and the FMA have also led the development of a financial sector New Zealand Cyber-Attack Response Protocol.[9] The Protocol will support financial sector agencies in responding in a more coordinated manner to cyber-attacks impacting regulated entities. This will complement the role of cyber agencies and the New Zealand's Cyber Security Emergency Response Plan (version 5, July 2021). Information obtained from our incident reporting requirements will be shared with the FMA and other relevant agencies (see further detail below) to support our supervisory engagement relating to a cyber incident.

[8] The FMA's notification requirement relates to any event that materially impacts the operational resilience of a financial institutions critical technology systems.
[9] Quarterly Statement by the Council of Financial Regulators – May 2022 | Kaunihera Kaiwhakarite Ahumoni - Council of Financial Regulators (cofr.govt.nz)

We also propose that information we collect through the two periodic surveys will be shared with the FMA to inform our respective work on the cyber resilience of our regulated entities.

## 5.3 Working with other cyber agencies

We aim to maximise the value of our cyber data collection and minimise compliance costs associated collecting this data. In addition to working closely with the FMA, we also collaborate and coordinate with other relevant agencies including the National Cyber Security Centre (NCSC) and the Computer Emergency Response Team New Zealand (CERT NZ). 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. We also collaborate with Australian Council of Financial Regulators agencies in the event of an attack impacting an entity operating in both countries (e.g. one of the large trans-Tasman banks).

## 5.4 Other information gathering initiatives

In our previous cyber consultation, submitters have 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 acknowledge 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 because they help improve knowledge across industry about responding to cyber-attacks. We do 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.

The Reserve Bank is also aware that the NCSC has surveyed the financial sector's resilience in the past[10] and is preparing for future regular resilience surveys. The Reserve Bank and NCSC are working together to understand the information requirements of both parties in order to identify where collaboration may be possible to reduce duplication for regulated entities. This approach reflects feedback that has already been received from the NCSC Finance Sector Information Exchange – although membership of this forum is only a subset of Reserve Bank regulated entities.

The Reserve Bank understands that the NCSC will continue to seek further engagement with organisations independently to explore in more detail issues that are covered through this survey. It is important to ensure the ongoing exchange of cyber security information with the NCSC that any information shared directly with the NCSC remains confidential and will not be shared. The NCSC may assist the Reserve Bank in the development of data collection questions, based on its situational awareness, but will not provide organisation-specific information.

The Reserve Bank seeks feedback on the proposal to share the full detail of its cyber resilience data collection with the NCSC to deliver more accurate information and present a unified effort, mitigating risk of loss of confidence in the financial system due to cyber attacks. The NCSC provides services that assists nationally significant organisations in the identification and management of cyber security risk. Data on the relative maturity of organisations and the uptake of guidance enables these services to be provided on a prioritised basis. Feedback is sought on

[10] https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Resilience-Assessment.pdf

the comfort of regulated entities on the Reserve Bank and NCSC having shared access to this data or suggested controls.

| | |
|---|---|
| **Q7** | Do you have comments on how we propose to share information? |

## 5.5 Legal basis for the collection of information

In our relevant sectoral legislation the Reserve Bank has powers to collect information for a range of purposes. Our cyber data collection proposals will be collected under these authorities. The relevant legislation is:

- Section 93 Banking (Prudential Supervision) Act 1989;
- Section 121 Insurance (Prudential Supervision) Act 2010; and
- Section 47 Non-bank Deposit Takers Act 2013.

Collected information must be kept confidential in accordance with applicable confidentiality provisions. These are:

- Section 105 Banking (Prudential Supervision) Act 1989;
- Section 135 Insurance (Prudential Supervision) Act 2010; and
- Section 54 Non-bank Deposit Takers Act 2013.

The confidentiality provisions permit the Reserve Bank to share information with the FMA and law enforcement or regulatory agencies in certain circumstances.

# 6 Financial Policy Remit

In undertaking our functions as prudential regulator we are required to have regard to the financial policy remit. A full discussion of the financial policy remit is included in Annex C. The proportionality and cyber resilience components of the remit are of higher relevance for the proposals in this consultation paper:

- *Proportionality:* we have considered proportionality in proposing the periodic reporting requirements. In particular, we propose a tiered approach to the period for reporting cyber incidents between large and other regulated entities. Consultation will also be an opportunity to test the balance of these requirements.
- *Improved cyber resilience:* the proposals in the consultation paper will directly contribute to this component. They will improve our understanding of the cyber risks facing our regulated entities and will also enable closer work between financial regulators and our regulated entities in the event of a cyber incident impacting a regulated entity (through improved information flows).

| | |
|---|---|
| **Q8** | Do you have any comments on our analysis on the financial policy remit? |

# 7 Next Steps

Following consultation, the Reserve Bank intends to implement the incident reporting requirements as the first priority of the proposals in the consultation paper. This will support enhanced incident response by the Reserve Bank and contribute to the Reserve Bank's role in supporting enhanced coordination. We anticipate working towards implementation as soon as possible this year.

We anticipate that the information gathering Cyber Survey will be finalised later in 2023 to support our ongoing supervision of regulated entities and policy insights over the longer term. The exact timing though of an initial survey is still to be determined.

| | |
|---|---|
| **Q9** | Do you have comments on our proposed prioritisation of our cyber data collection proposals? |

# 8 Consultation questions

Your feedback is important. This consultation provides you with the opportunity to give your views on, and any information relevant to, our proposed cyber data collections. The main text of this Consultation Paper includes some questions you may wish to respond to. A consolidated list of the questions is set out below. Comments do not need to be made in respect of all the questions. You may focus on those areas that are of most importance to you. Comments are welcome on any other matters you consider relevant to our cyber data collection proposals.

## 8.1 Questions

| | |
|---|---|
| **Q1** | Do you have comments on our proposed cyber incident reporting timeframe? |
| **Q2** | Do you have comments on our proposed definition of materiality? |
| **Q3** | Do you have comments on our proposed cyber incident reporting template? |
| **Q4** | Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting? |
| **Q5** | Do you have comments on our proposed periodic cyber resilience capability survey? |
| **Q6** | Do you have comments on our proposed frequency of reporting? |
| **Q7** | Do you have comments on how we propose to share information? |
| **Q8** | Do you have any comments on our analysis on the financial policy remit? |
| **Q9** | Do you have comments on our proposed prioritisation of our cyber data collection proposals? |

## 8.2 Contact details

All responses should be emailed to cyberresilience@rbnz.govt.nz or sent to:

Cyber data collection consultation
Dynamic Policy
Prudential Policy Department
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

We welcome submissions until 5pm, 3 July 2023.

## Annex A: Draft Incident Reporting Template

The draft incident reporting template is an excel file available on the Reserve Bank's website.

# Annex B: Periodic Survey Questionnaire

This survey aims to establish the entity's level of cyber resilience based on the Reserve Bank Guidance on Cyber Resilience (referred to in questions as the Reserve Bank Guidance).

| A. Governance | | Data type |
|---|---|---|
| **A1. Board and Senior Management Responsibilities** | Q1. To what level is your organisation following the Reserve Bank Guidance for governance responsibilities of the Board and Senior Management? | Exceeds/Enhanced/Baseline/Partial |
| | Q2. Is there a dedicated Chief Information Security Officer or senior executive accountable for the cyber resilience strategy? | Yes/No |
| | Q3. If yes, how long has the Chief Information Security Officer (or senior executive accountable for the cyber resilience strategy) been in the role? | Numeric |
| | Q4. Number of scheduled and impromptu cyber briefs at Board meetings in the last 24 months? | Numeric |
| | Q5. Number of scheduled and impromptu briefings to executive management teams in the last 24 months? | Numeric |
| | Q6. Are internal audit results and incident near misses reported to the Board? | Yes/No |
| **A2. Cyber Resilience Strategy and Framework** | Q7. Does a Board approved cyber resilience strategy exist that is consistent with the Reserve Bank Guidance? | Fully/Mostly/Partially/Ad hoc |
| | Q8. Does a formally documented programme exist to maintain and increase your security posture and to deliver the cyber resilience strategy, consistent with the Reserve Bank Guidance? | Fully/Mostly/Partially/Ad hoc |

| A. Governance | | Data type |
|---|---|---|
| | Q9. Do you have an internal audit process to help monitor and measure the implementation progress, adequacy and effectiveness of the cyber resilience strategy and framework programme? | Fully/Mostly/Partially/Impromptu |
| | Q10. How frequently is the cyber resilience strategy and framework programme reviewed and updated? | Years |
| **A3. Culture and Awareness** | Q11. What percentage of staff completed the relevant cyber training events/ modules over the past 12 months? | Numeric |

| B. Capability Building | | Data type |
|---|---|---|
| **B1. Identify** | Q1. To what level is your organisation following the Reserve Bank Guidance for capability building (Identify)? | Exceeds/Enhanced/Baseline/Partial |
| | Q2. Have critical functions that your organisation relies on (including internally and external supported, both customer facing and non-customer facing systems) been identified? | Yes/No |
| | Q3. What is the number of critical functions with unacceptable risk levels? | Numeric |
| | Q4. How many cyber risk assessments have been conducted in the last 12 months on new or existing/updated technologies, products, services or processes in order to identify any associated threats or vulnerabilities? | Numeric |
| | Q5. How many critical functions are currently overdue their risk assessment period? | Numeric |

| B. Capability Building | | Data type |
|---|---|---|
| **B2. Protect** | Q1. To what level is your organisation following the Reserve Bank Guidance for capability building (Protect)? | Exceeds/Enhanced/Baseline/Partial |
| | Q2. How many staff have privileged access to systems and information (noting the principle of least privilege)? | Numeric |
| | Q3. How often is this information audited? | Years |
| | Q4. How many times have you recorded breaches of security controls in the last 12 months? | Numeric |
| | Q5. How many risk assessments have been undertaken? | Numeric |
| | Q6. How many of these risk assessments recommended new controls which have been implemented? | Numeric |
| | Q7. Is a security assessment undertaken as part of change management? | Yes/No |
| | Q8. How many times in the last 12 months have you assessed for cyber security risk (include data loss prevention, data egress checking, data classification)? | Numeric |
| **B3. Detect** | Q1. To what level is your organisation following the Reserve Bank Guidance for capability building (Detect)? | Exceeds/Baseline/Partial |
| | Q2. Are anomalous activities and events being monitored and reported on? | Yes/No |
| | Q3. How many internal staff are trained to be able to identify anomalous activities and events? | Numeric |
| | Q4. How many times were event, system, and data logs backed up to a secure location over the last 24 months? | Numeric |

| B. Capability Building | | Data type |
|---|---|---|
| | Q5. What is the retention period of logs for critical systems? | Months/Years |
| | Q6. How many times was this information analysed over the last 24 months? | Numeric |
| | Q7. How regularly, in the last 12 months, were security tests conducted on systems and networks to detect weakness that could be exploited by a cyber-attack? | Numeric |
| | Q8. Were security tests also undertaken with all major changes in new systems or technologies? | Yes/No |
| **B4. Respond and Recover** | Q1. To what level is your organisation following the Reserve Bank Guidance for capability building (Respond and Recover)? | Exceeds/Enhanced/Baseline/Partial |
| | Q2. Do you have a response and recovery plan for when a cyber-breach occurs (in line with the recommendations of the Reserve Bank Guidance)? | Yes/No |
| | Q3. If yes, when was the response and recovery plan last updated? | Months/Years |
| | Q4. Do you use scenario testing (i.e. table-top exercise) to stress test your recovery plan? | Yes/No |
| | Q5. Do have a process in place that incorporates lessons learned from cyber scenarios and incidents? | Yes/No |
| | Q6. Do you have a communications plan in place to notify external stakeholders? | Yes/No |
| | Q7. When was the communications plan last reviewed? | Months/Years |

| C. Information sharing | | Data type |
|---|---|---|
| **C1. Channels** | Q1. To what level is your organisation following the Reserve Bank Guidance for information sharing? | Exceeds/Baseline/Partial |
| **C2. Process** | Q2. Is your organisation following the baseline recommendations in the Reserve Bank Guidance for information sharing? | Fully/Mostly/Partially |
| | Q3. Do you have the capability to share anomalous activities and events detected? | Yes/No |

| Part D: Third-party management | | Data type |
|---|---|---|
| **D1. Planning** | Q1. Who are your third party providers of critical functions and what services do they provide? | Please list. |
| | Q2. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Planning)? | Exceeds/Enhanced/Baseline/Partial |
| **D2. Due diligence** | Q3. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Due diligence)? | Exceeds/Enhanced/Baseline/Partial |
| **D3. Contract negotiation** | Q4. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Contract negotiation)? | Exceeds/Enhanced/Baseline/Partial |
| **D4. Ongoing cyber risk management** | Q5. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Ongoing cyber risk management)? | Exceeds/Enhanced/Baseline/Partial |
| **D5. Review and accountability** | Q6. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Review and accountability)? | Exceeds/Enhanced/Baseline/Partial |

| Part D: Third-party management | | Data type |
|---|---|---|
| **D6. Documentation** | Q7. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Documentation)? | Exceeds/Baseline/Partial |
| **D7. Termination** | Q8. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Termination)? | Exceeds/ /Baseline/Partial |
| **D8. Outsourcing to Cloud Service Providers** | Q9. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (Outsourcing to Cloud Service Providers)? | Exceeds/ Baseline/Partial |

| Part E: Resources | | IT % of overall entity |
|---|---|---|
| **E1. Total Organisation Headcount**<br><br>*Basis of measure: Full time equivalent employees and third-party IT providers.* | *Headcount information provides RBNZ with a way of characterising what human resourcing is available to manage, maintain, change and operate its IT systems. The data will provide a benchmark/baseline and range as a % of allocated headcount of the entity.*<br><br>***Third Party IT providers***<br><br>*For the purposes of this question, third party IT providers are independent entities which provide greater than 10% of internal IT personnel to the regulated entity.* | |
| **E2. Headcount of information security (IT) personnel (excluding board and senior management)**<br><br>*Basis of measure: Full time equivalent employees and contractors.* | Basis of measure: Full time equivalent employees and contractors. Limit to personnel with a dedicated information security role. | |

# Annex C: Financial Policy Remit

The Financial Policy Remit emphasises the desirability of a strong, efficient and inclusive financial system, with a low incidence of failure of regulated entities. It also signals that we should encourage a competitive financial system and have regard to Government priorities on sustainable house prices, building resilience and facilitating adaption to climate change, improving financial inclusion, and improving cyber resilience. This section outlines a summary of how we have had regard to the Financial Policy Remit in the policy proposals in this paper. The full text of the Remit is available on the Reserve Bank's website.[11]

## Summary of Analysis

We consider two components of the remit to be of particular relevance to the cyber data collection proposals.

First, the 'improving cyber resilience' component of the remit is of high relevance. These proposals are specifically designed to inform our understanding of the cyber resilience of individual entities, as well as the cyber resilience of our regulated entities as a whole. Collection of this information will directly contribute to supporting the Reserve Bank, and other financial regulators, in monitoring and supervising the cyber resilience of our regulated entities.

Secondly, while cyber risk is relevant for all regulated entities, there is greater risk posed (particularly for the wider financial system) from large financial institutions. Recognising this spectrum, we consider the proportionality component of the remit to also be of relevance. To ensure a proportionate approach, we propose different reporting timeframes between large entities and other entities. This is intended to reduce the compliance costs for smaller entities that pose relatively smaller risk for the financial system as a whole.

The table below outlines the components of the Financial Policy remit that are relevant for this paper, and summarises the expected impacts. It outlines how these components have been given regard to and their relative weight for consideration.

| Component of the Financial Policy Remit | Summary of analysis and relevance to proposals in this paper |
|---|---|
| "It is desirable to have a financial system that is strong, efficient and inclusive, with a low incidence of failure of entities regulated by the Reserve Bank." | This component is not of high relevance. However, improving the cyber resilience of entities will contribute to reducing the risk of failure or significant outages as a result of operational failure of an entity or liquidity issues that could arise within the financial system as a result of a significant cyber incident. |
| "Within the appetite of a low incidence of failure, a competitive financial system should be encouraged so as to best ensure ongoing financial efficiency and inclusion." | This component is not of high relevance. The proposals in this paper are not expected to impose significant costs that could provide barriers to entry and inhibit competition. More generally, there is a compliance cost for entities in ensuring their cyber resilience through putting in place adequate risk management systems. However, adequately managing cyber risk is important |

[11] The text of the Financial Policy Remit is available on the Reserve Bank's website: https://www.rbnz.govt.nz/about-us/responsibility-and-accountability/our-financial-policy-remit

| Component of the Financial Policy Remit | Summary of analysis and relevance to proposals in this paper |
|---|---|
| | for ensuring the soundness of financial institutions given the important role they play in the New Zealand economy. |
| "imposing regulatory and supervisory costs that are proportionate to the expected risks and benefits to the financial system and society" | Proportionality is a consideration of importance for this proposal; paragraphs 15-16 discuss the proposed approach. |
| "encouraging new investment and financial innovation that raise the productive potential of the economy" | This component is not of high relevance to these proposals. |
| "encouraging the allocation of financial resources in a way that maximises the sustainable long-term growth of the New Zealand economy" | This component is not of high relevance to these proposals. The proposals do not impact the way in which financial institutions allocate funding. |
| Sustainable house prices | The proposals in this paper are not expected to have a significant impact on sustainable house prices. This component has been given a low weighting for consideration in our analysis. |
| Building resilience and facilitating adaption to climate change | The proposals in this paper are not expected to have a significant impact on climate change. This component has been given a low weighting for consideration in our analysis. |
| Improving financial inclusion | The proposals in this paper are not expected to have a significant impact on financial inclusion. This component has been given a low weighting for consideration in our analysis. |
| Improving cyber resilience | The proposals in this paper are expected to have a material impact on improving cyber resilience and the Reserve Bank's understanding of incidents as they happen. The proposed data collection is the second step in the Reserve Bank's three step policy approach to supporting improved cyber resilience in our regulated entities. The information collected will improve the Reserve Bank's understanding of the cyber resilience of the financial sector. It will provide for better informed policy and supervisory approaches to enhance cyber resilience; and improved incident response by both the Reserve Bank and other financial regulators. |