Reserve Bank of New Zealand
Te Pūtea Matua

Cyber Resilience Data Collection.

Summary of Submissions and Key Decisions

4 March 2024

Table of Contents

Background 2
Consultation Process 2
Summary of Submissions 3
General comments 3
General views and concerns 3
Reserve Bank's Response 3
Material cyber incident reporting (Q1-Q3) 3
Q1: Do you have comments on our proposed cyber incident reporting timeframe? 3
Reserve Bank's Response 4
Q2: Do you have comments on our proposed definition of materiality? 5
Reserve Bank's Response 6
Q3: Do you have comments on our proposed cyber incident reporting template? 7
Reserve Bank's Response 9
Periodic cyber incident reporting (Q4) 11
Q4: Do you have comments on our proposed periodic reporting of cyber incidents and/or the frequency of reporting? 11
Reserve Bank's Response 12
Cyber capability survey (Q5-Q6) 13
Q5: Do you have comments on our proposed cyber capability survey? 13
Reserve Bank's Response 14
Q6: Do you have comments on our proposed frequency of reporting or the threshold for reporting more frequently? 15
Reserve Bank's Response 15
Information sharing, financial policy remit and policy prioritisation (Q7-Q9) 15
Q7: Do you have comments on how we propose to share information? 15
Reserve Bank's Response 16
Q8: Do you have any comments on our analysis on the financial policy remit? 17
Reserve Bank's Response 17
Q9: Do you have comments on our proposed prioritisation of our cyber data collection proposals? 18
Reserve Bank's Response 18
Annex 20
A1. Changes to the Material Cyber Incident Template Instructions 20
A2. Summary of changes to the Material Cyber Incident Notification Report Template 21
A3. Cyber Capability Survey Cover Pages 26
A4. Changes to the Cyber Capability Survey Template 26

Background

Cyber risk – both malicious and non-malicious – is expanding 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. Thus, building and maintaining cyber resilience is important to promote a sound and dynamic financial system.

The Reserve Bank of New Zealand – Te Pūtea Matua (the Reserve Bank) has been undertaking a 3-step approach to supporting building cyber resilience in our regulated entities. These steps are: Cyber Risk Management Guidance (Step 1, published in Q2 2021); Cyber Data Collection Requirements and Information Sharing Arrangements (Step 2 – this paper); and Enhanced Coordination and Response to Cyber Incidents (Step 3 – completed in 2022).

As part of the Step 2 of our policy approach, the Reserve Bank consulted on cyber data collection proposals in mid-2023. The consultation document proposed the following data collection requirements for Reserve Bank regulated entities, except for financial market infrastructures (FMIs), which have separate requirements:

- A material cyber incident reporting requirement: This is a requirement to report to the Reserve Bank material cyber incidents as soon as practicable, but within 72 hours. This requirement is intended to support engagement between the Reserve Bank and regulated entities in the event of a material cyber incident.

- A periodic reporting of all cyber incidents: This is a requirement to report to the Reserve Bank all cyber incidents regardless of materiality. This requirement aims to provide a holistic view of the cyber risks that regulated entities face.

- A periodic survey on the cyber resilience of regulated entities: This is a requirement to respond to the Reserve Bank's cyber capability survey. This requirement aims to improve our understanding of the finance sector's resilience to cyber threats at individual and sector-wide level. It will also inform our supervisory engagement with individual entities on their cyber resilience.

Consultation Process

The consultation opened on 8 May 2023 and closed on 3 July 2023. Fourteen submissions were received, of which 5 came from industry bodies, 8 from companies and 1 from an individual (Table 1). The 5 financial market organisations are Corporate Trustees Association, Financial Services Federation, New Zealand Banking Association (NZBA), Insurance Council of New Zealand and Financial Services Council New Zealand. The 8 respondent companies are comprised of 3 banks, 2 insurance companies, 1 non-bank deposit-taker, and 2 technology companies.

Table 1: Consultation respondents by type of entity

Type of respondent	Number
Industry body	5
Bank	3
Insurance company	2
Non-bank deposit taker	1
Other company	2
Individual	1
Total	**14**

We additionally had bilateral discussions with industry stakeholders during the consultation period.

This document summarises the submissions received in response to our consultation and our responses to the points raised in these submissions. The discussion focuses on the common themes and views and is not intended to be an exhaustive account of all the points raised. Notably, not all respondents expressed views on all the issues consulted.

Summary of Submissions

General comments

General views and concerns

Respondents generally expressed support for the direction of the Reserve Bank's work on cyber resilience. They recognised the impetus of our initiative to collect relevant cyber incident information to better understand the cyber risks and supported our proposed approach to work closely with the Financial Markets Authority (FMA) to make the reporting requirements consistent.

Respondents' comments mainly focused on the definitions of some of the terms in the consultation paper, level of detail required in the reporting templates, incident reporting format (i.e. with some suggesting alternative reporting formats to Excel), reporting frequency, compliance with similar requirements of other agencies and data security.

Reserve Bank's Response

We welcome the support of our efforts to collect more information on cyber incidents considering the growing importance of cyber resilience as an area of operational risk. We appreciate the feedback received on the detail of our proposals and agree that there are some areas where we can streamline our proposed approach to the reporting of material cyber incidents and the level of information collected in the cyber capability survey to make the collection process more efficient and better focus the information collected. Our proposed changes in response to feedback from submitters are outlined in the responses to specific questions discussed below.

Material cyber incident reporting (Q1-Q3)

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

Respondents generally agreed with or did not oppose to the proposed 72-hour window to report a material cyber incident although a respondent expressed concern about the practicality of providing the requested information within the suggested period.

A number of respondents sought clarification on the precise definition of the 72-hour timeframe (i.e. whether it includes non-business hours, public holidays and weekends). There were also questions as to when "detection" starts (i.e. if it starts before or after the materiality has been established), with a number of respondents proposing that it should begin when the materiality of the incident has been established.

Separately, respondents sought clarification if updates have to be submitted if such updates are deemed to be not material and guidance on how the reporting timeline of this requirement aligns with the timeline of operational incidents not caused by cyber attacks. They also asked for

confirmation as to whether the incident response template can be used to report both material cyber incidents and material operational incidents to avoid performing multiple assessments for the same cyber incident for reporting purposes.

On the level of detail of the template, some respondents considered it to be excessive. A number of respondents also expressed that completing Part B every 24 hours would be burdensome. To facilitate ease in compliance, at least 1 respondent proposed that our reporting requirement:

- Gives smaller entities longer timeframes in recognition of their capacity and the risk they pose to the financial system;
- Makes the reporting timeframes more pragmatic (i.e. open communication rather than point in time reporting) and flexible (e.g. in cases wherein the systems that hold the required data are impacted);
- Allows for Part A to be partially completed and submitted initially, and gives the entity more time to complete it in the event of non-malicious and isolated cyber incident;
- Allows for Part B to be provided on a weekly basis or as information becomes available, and requires immediate updates only in the event of a malicious widespread incident; and
- Clarifies the mechanism for changing the classification of an incident (e.g. upgrading or downgrading the classification) once further information has become known to expedite reporting.

Reserve Bank's Response

Our proposed cyber reporting timeframe seeks to balance timely information reporting with sufficient flexibility for the range of cyber incidents that may occur and of size of entities regulated by the Reserve Bank. Additionally, the timeframe aligns with APRA's cyber incident reporting timeframes and the FMA's incident reporting timeframe for financial institutions. We consider that alignment of reporting timeframes avoids confusion with requirements across different regulatory regimes or jurisdictions.

We note that while the 72-hour window is intended to accommodate a wide range of entities and diverse nature of cyber incidents, we expect entities to contact their supervisors as soon as practicable rather than waiting for complete information. We recognise that it is possible that the initial information provided may be incomplete or may change as further information regarding the incident is ascertained.

We define "detection" to start at the time when the materiality of the cyber incident has been established, which is consistent with APRA's definition. Accordingly, the 72-hour timeframe pertains to consecutive hours, which include non-business hours, public holidays and weekends. This definition is consistent with APRA's definition and recognises that cyber attacks can happen at any time of the day and on any day of the week.

With regard to the reporting cadence for Part B, it is not our intention to add another process in reporting an incident. We also acknowledge that the frequency of reporting may need to vary through the course of an incident. It is our expectation though that entities will keep the Reserve Bank regularly informed as necessary. We have updated the instructions page of the template to specify how Part B should be used. In particular, we:

- Clarified that updates are to be provided regularly rather than at a set period (i.e. this could align with the internal practice of reporting incidents to an entity's senior management and their board);

- Streamlined the required fields in the template and provided options on the manner of reporting the update (as detailed in our response under Q3); and
- Clarified that regular updates need to be provided through the course of an incident regardless of the nature of the internal categorisation of the updates themselves. Please refer to our comments on the definition of "materiality" in the next section.

Meanwhile, changes to the severity classification of the incident can be indicated in the responses to questions B07.0 and C07.0 of the template. This is discussed further in our response to the comments to Q3.

We additionally confirm that the template can be used for reporting on both the Reserve Bank's material cyber incident requirements and the FMA's reporting requirements for events that materially impact the operational resilience of critical technology systems. It can also be used to report material cyber incidents and material operational incidents.

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

Respondents who have expressed their opinions on this question were generally supportive of the proposed definition and welcomed the approach of aligning our definition with APRA's.

However, the majority of the respondents asked for guidance in determining the materiality of incidents (including if contractual or legislative breaches are included and how non-financial impact is considered). Some respondents suggested that examples of incidents that meet the materiality threshold or benchmarks be provided as reference. Respondents requested for definitions of "cyber event," "cyber incident," "cyber attack," "cyber resilience" and "cyber security."

Notably, some respondents considered that our definition is broader than FMA's which will likely result in substantive differences in the types of incidents reported. At least 1 submission also noted that in contrast to our definition, system participants and prudential concerns are not part of the materiality definition in APRA's CPS 234.

In this regard, some respondents proposed that we align our definition with the definitions of other New Zealand regulatory agencies, such as FMA and the Office of the Privacy Commissioner, to avoid having regulated entities perform multiple assessments for the same incident. A respondent likewise suggested that we consider a tool, such as the Office of the Privacy Commissioner's "NotifyUs," to help with triaging and to provide guidance on the need to report.

Accordingly, several submissions sought for guidance in determining whether the cyber incident has "the potential to materially affect, financially or non-financially, the entity or the interests of its stakeholders." We also received submissions that proposed to remove this phrase from our definition of materiality for them to focus on material cyber incidents that transpired.

The respondents further asked us to:

- Clarify whether there is an intention to link this to the subsections of Section 78 of the Banking (Prudential Supervision) Act 1989 which covers "Carrying on Business in Prudent Manner" or whether there is a different set of considerations;

- Consider removing the line "the extent to which the cyber incident could result in financial consequences to the New Zealand financial system or to other financial entities" from the guidance because it is difficult for financial institutions to ascertain the impact on the financial system or other financial entities;

- Consider removing the question "how long the cyber-incident lasted (if already remedied) or is expected to continue" in assessing materiality because there may be instances when the immediate disruption of the cyber incident is mitigated and ongoing impact is minimised even if the affected entity continues to remedy the incident; and

- Clarify how to calculate the length of incident if the above question is retained, to which the proposal is to exclude post-incident efforts, such as root-cause analysis, controls uplift, and others.

Reserve Bank's Response

First, we note that our definition of material cyber incident should be interpreted consistently with the glossary of the Reserve Bank's Cyber Resilience Guidance. The glossary reflects the cyber lexicon of the Financial Stability Board (FSB), which contains relevant definitions for interpreting the material cyber incident definition. We consider that there is value in maintaining alignment with the FSB lexicon.

Notably, FSB has updated its cyber lexicon in April 2023. We note in particular the changes to the definition of "cyber incident." We also note that the definition of "material cyber incident" is revised to exclude the phrase "… system participants, or more broadly raises prudential concerns." This will align our definition with APRA's definition, which we consider appropriate given our common roles as prudential regulators.[1] The above-quoted phrase was initially intended to capture FMIs. However, separate requirements have now been put in place for FMIs.

On the comments that we align our definition with FMA's, we note that our definitions have substantial overlaps.[2] Nonetheless, given that our objectives are not entirely the same, marginal differences in definitions cannot be completely avoided. At the same time, the similarities in objectives underpinned our decision to align our definition with APRA's.

In response to other additional comments, we confirm that this data reporting requirement supports the intent of Section 78 of the Banking (Prudential Supervision) Act 1989 requiring registered banks to carry on their business in a prudent manner. This reporting requirement, however, mainly considers data and cyber system protection controls. Given the current context, this has become a key prudential regulation dimension that covers bank and non-bank entities (i.e. includes NBDTs and insurance companies).

In assessing whether incidents meet the materiality threshold or benchmarks or could potentially materially affect, financially or non-financially, the entity or the interests of its stakeholders and examples of such incidents, we refer the respondents to the consultation paper for guidance (pages 10-11).

On the elements cited to assess the materiality of the incident (page 11 of the consultation document), we consider that the criteria relating to "the extent to which the cyber incident could result in financial consequences to the New Zealand financial system or to other financial entities" and "how long the cyber-incident (if already remedied) or is expected to continue" are necessary. Thus, we intend to maintain these as part of the guidance.

We understand that the answers to these guidance questions may not be precise and the thresholds can, at times, be subjective. However, the element of subjectivity cannot be avoided in

[1] See APRA (2019), Prudential Standard CPS 234 Information Security, line 34 (a).
[2] See: FMA (2022), Cyber Security & Operational Systems Resilience, page 6 (Reporting) for FMA's definition of incidents that are required to be reported.

setting the guidance to assess the materiality of the incidents. The subjectivity of responses (to some degree) also does not nullify the relevance of the guidance question. Moreover, these guidance elements are not necessarily new as they were drawn from the Reserve Bank's framework for breach reporting for registered banks.

On the question on how to calculate the duration of the incident, the entity can consider the point when the incident materiality has been established as the starting point (as noted in our response to the Q1 feedback) and the point when the incident is considered to have ended by the IT or an equivalent team within the organisation as the end point (consistent with the Part C submission). We clarify that the entity should exclude post-incident efforts in the calculation of the duration after the incident has been considered to have ended, although the entity can detail these efforts in their Part C submission.

Q3: Do you have comments on our proposed cyber incident reporting template?

The respondents were broadly supportive of the template and appreciated the proposal that the incident notification template be used for reporting to both the Reserve Bank and FMA. Nonetheless, there were substantive comments on the level of details and on the relevance of collecting some of the information in the template. There were also questions and suggestions relating to reporting format, information security, frequency of submissions and some specific line items.

Level of information

General comments

Some respondents noted that the proposed template is too complex and more detailed compared to the reporting requirements of the other New Zealand agencies (e.g. OPC, CERT NZ and NCSC) and APRA. They further conveyed that it is not practical to gather the required details during an initial incident response and remediation with a tight timeframe because it will distract the entity's response and recovery efforts, especially given that not all the information requested is readily available.

A number of respondents separately opined that the proposed level of details does not necessarily position the Reserve Bank to mitigate cyber incidents since it does not provide technical response to incidents.

Given these concerns, some respondents suggested that the template be streamlined to include only key information or provide an option for financial institutions to fill out the template to the best of their knowledge. At least 1 respondent also proposed to include a section in the template where the cyber incident can be described by the entity to appropriately capture the context in addition to the drop-down options and boxes for short answers. Meanwhile, a respondent wanted finer granularity for known first detection, including a MITRE ATTACK reference if possible and the method for determining the incident.

Regarding the framework, a respondent requested that we consider FSB's format for incident reporting exchange (FIRE) and wait for the final FSB template before introducing our own. Its submission conveyed that given the high degree of commonality in the types of cyber incident information that financial institutions are required to report to different regulators, alignment with the FSB format allows reporting entities to streamline the process of generating the information that are required from them.

To avoid duplication of reporting a similar incident or update to multiple regulators, some respondents expressed preference towards establishment of a single point of contact or central agency, which can be the Reserve Bank or another government agency. Respondents also clarified if parts A, B and C must be submitted together with each subsequent submission, which can be repetitive.

Comments to Part A

Some respondents proposed that Part A be streamlined and refined. One respondent commented that many of Part A questions would only be available during the post-incident review (PIR) process in many organisations. APRA's 72-hour notification, which the respondents described as a short form with high-level questions about the incident and mitigating actions taken, is suggested as a reference. The webform used by the Australian Cyber Security Centre was also mentioned in the submissions for consideration.

Specific proposals to refine Part A were: including the option "inappropriate use" in A08.0 drop-down list to capture incidents due to internal human error and/or employee malicious behaviour; removing "occasional IT outages" in A09.0 from cyber incident reporting; amending "distributed denial of service attacks" (DDOS) in A08.1, B08.1 and C08.1 to "Denial of service attacks," which encompasses DDOS, to align with the categorisation used by the NCSC and CERT NZ; adding "All" as an option in A14.1; deleting A17.0 as it is subjective; and adding NBDT supervisors in the A20.0 list as NBDTs need to report material issues to them.

Moreover, some respondents queried the definitions of "Active/Under investigation/Mitigated" in A06.0 and "regulatory impact" in A18.0, which is noted to be a surplus question as this is also raised in A20.0. Respondents likewise questioned the purpose "Low" severity classification (A07.0) that seems to entail that the incident does not meet the materiality threshold and seek guidance on whether "cyber attack" in A08.0 refers to the cause of the "internal outage/service failure" in A09.0.

Comments to Part B

General feedback regarding Part B included streamlining the form; not requiring submission every 24 hours and reserving it for material new information until the cyber incident has concluded and has been fully mitigated and resolved; and removing it from the template altogether.

Several respondents expressed preference for open communication with their respective supervisors in providing updates and in determining the next steps after the Reserve Bank is made aware of the incident. One submission stressed that requests for further information should be from either the Reserve Bank or FMA and not both, and adds that if an incident affects more than 1 regulated entity that is required to report to the Reserve Bank, the entities should have the option to elect for 1 entity to provide the report on behalf of all affected entities.

Some respondents noted that fully completing Part B in every update will make it burdensome for the Reserve Bank to manually identify the new or amended information.

Comments to Part C

Furthermore, some respondents considered that Part C requires detailed and sensitive information that if sent externally poses a risk to regulated entities. The respondents suggested that conclusions are discussed with the supervisors instead. Meanwhile, at least 1 respondent suggested

that if the incident is resolved within 72 hours, the reporting entity should only submit Part A within 72 hours and not Part C.

Reporting file format

The reporting file format is the second key issue that the respondents raised. The respondents noted that Excel is not a secure format given its inadequate encryption features to protect sensitive business information. They emphasised the need to encrypt the incident report submissions while Excel is prone to errors and presents scalability and collaboration difficulties. At least 1 respondent further queried the benefits of maintaining open channels of communication during an incident as previously enacted were assessed against the use of Excel spreadsheet.

In lieu of Excel, some respondents suggested an online incident reporting similar to what CERT NZ, OPC and APRA have in place for their regulated entities.

Reserve Bank's Response

Our template is designed and intended to be used by a range of different entities. There is a balance to be struck in providing specificity which may be helpful in guiding reporting for smaller entities and rigidity for larger entities that may have more comprehensive existing internal reporting systems. We consider that our proposed structure of the reporting template remains appropriate, but we agree that the template can be refined to improve useability. We have streamlined all 3 parts by consolidating or deleting some questions considering the feedback received on the level of details.

For Part A, the information to be collected is focussed on understanding the impact of the cyber incident. The information requested should be substantially available to the entity within the reporting period. Before detailing the changes, we note that we have considered requirements in other jurisdictions including APRA's 72-hour notification requirement in deciding the information that included in Part A.

We have made the following key changes/clarifications to the template[3]:

- We deleted the question on the current status of the incident, i.e., whether "Active/Under investigation/Mitigated" in the revised template (A06.0). We take that submission of Parts A means that the incident is active and under investigation.

- We removed the "Low" severity classification under question A07.0 since low classification entails that the incident does not meet the materiality threshold and would therefore be beyond the scope of this reporting requirement. However, we kept this option in Parts B and C (i.e. questions B07.0 and C07.0) in case the reporting entity downgrades the classification of the incident as mentioned above. We clarify, however, that in cases when the incident severity classification is downgraded to "low" in the entity's Part B report, we still expect the entity to submit updates until the incident is resolved. Downgrading of the incident severity classification to low should not be construed to mean incident resolution.

- We added "both" as an option in the revised template if the incident happens to be a cyber attack resulting in 'internal outage/service failure' (A08.0 and A09.0). Hence, the entity can submit the same material cyber incident report to cover a material cyber

[3] The question codes mentioned in this report refer to the codes in the templates that were published for consultation unless otherwise clarified. These codes were changed in the revised templates as some questions in the consulted templates were either deleted or merged. For minor edits/changes to the questions or terms, refer to Annexes A1 and A2.

incident and material operational incident that are related (See our response to Q1 feedback). However, if the material cyber incident is independent from the material operational incident the reporting entity is expected to report these incidents separately. We also provided a definition for the term 'internal outage/service failure'. The same goes for items B08.0-B09.0 and C08.0-C09.0.

- We replaced the term "Distributed denial of service attacks" (DDOS) in A08.1, B08.1 and C08.1 with "Denial of service attacks" as suggested to align with the categorisation other agencies.

- We defined 'regulatory impact' (A18.0) in the revised template. We decided to keep this question to be clear whether the entity recognises that the incident has regulatory impact.

- We linked question A18.0 with A20.0 to be clear that we want to be informed if certain regulatory agencies have been notified of the incident notwithstanding the entity's view of the regulatory impact of the incident.

- We merged the questions on identification of viable solution (A21.0-A21.1, B21.0-B21.1, C21.0-C21.1) and actions taken to prevent further impacts (A19.1, B19.0, C19.0) to streamline responses on these questions given potential overlap.

Similar to Part A, we have clarified how we expect Parts B and C to be completed.

We agree with the respondents that greater flexibility could achieve receiving substantially the same information flow while providing entities choice on the best information flow in the course of an incident. In this regard, we have amended the template instructions by indicating that internal reporting can be utilised to satisfy the requirements of Part B. Part B can still be utilised by entities for whom the standardised approach may support easier reporting. It can also be used as guidance if the entity decides to use a different template.

For Part C, we have outlined greater flexibility in the extent to which Part C is completed. Where available, we have provided the reporting entity with an option to simply lift passages from the post incident report (PIR) in response to some line items if the information requested in the template is already in the PIR that the entity has submitted or will submit to the Reserve Bank.

In addition to the changes mentioned above, we made the following key changes to Parts B and C of the template:

- We replaced the questions on the current status of the incident in Parts B and C (B06.0, C06.0) with a question on whether the severity classification has changed since the entity's previous reporting. As above, we take that submission of Part B means that the incident is active and under investigation while submission of Part C means that the incident is resolved or mitigated.

- We deleted the questions that ask to describe additional actions taken to prevent further impacts (B19.1, C19.1) as these are already captured by other questions (B21.1, C21.1).

- We deleted the question that asks for duration estimate until the interruptions to services conclude (C22.0) because we have a separate question on when exactly the reporting entity expects the interruptions to conclude (C22.1), making the former redundant.

- We have provided the definitions for the terms 'conclusion of event/incident' (C22.1', 'interruptions to service' (C22.1), 'resolution of event/incident' (C23.0) and 'recovery time' (C24.0).

- We added a question in Part C on who is responsible for the review of the report and explicitly note atop that the respondent may lift parts of their PIR to respond to the questions.

We also clarify that if the material cyber incident is resolved within the 72 hours following identification, the entity is expected to complete Part A and the Conclusion section of Part C.

Annex A1 and A2 summarise the changes to the material cyber incident template. The revised material cyber incident template is posted on the Reserve Bank's website.

On the comment regarding FSB's Format for Incident Reporting Exchange, we are aware of this work.[4] We agree that it could a useful basis for reporting. However, this format is still being developed and may take time to finalise. The growing risk of cyber means that we cannot wait for this work to be completed to put in place more formal reporting requirements that the status quo. We will keep track of the project developments and consider the format once it is finalised.

We have considered the concerns of having to report to multiple agencies on the same incident. This is why we are coordinating with the FMA on possible information that can be shared to minimise the cost of compliance. However, considering the different mandates of the agencies involved, reporting cannot be entirely confined to a single agency. At the same time, we have to balance the intent of streamlining reporting with our data privacy and security obligations (as mentioned above) in sharing the information reported to us.

Regarding the manner of reporting and security requirements, we will utilise the Reserve Bank's secure file transfer service, BOX, to provide for the secure transfer of files to the Reserve Bank. We do not currently have the capability to put in place web-based reporting tools. Initiating discussions with supervisors concerning the incident is always welcome. In providing updates, entities may contact their supervisors. Nevertheless, we also consider it important to have these discussion points in report format, so we have decided to keep all 3 parts of the reporting template.

Periodic cyber incident reporting (Q4)

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

Some respondents conveyed that they do not see the relevance of the proposed periodic reporting and suggested that it should not be mandated. They questioned the idea of reporting non-material cyber incidents to the Reserve Bank and the alignment of doing so with international practice. They also noted that CERT NZ and NCSC are already collecting the same information and publishing periodic trend reports, and that APRA does not require reporting of all cyber incidents.

If this periodic reporting requirement were to be implemented, more than half of the respondents who expressed their views on this question agreed with the proposed frequency of reporting. One contention of those who disagreed to the proposed frequency was that the requirement to report all cyber incidents semi-annually for large entities and annually for all other entities is impractical

[4] See: FSB (2023), Format for Incident Reporting Exchange (FIRE): A possible way forward.

given that the volume could be large. Annual reporting, as opposed to semi-annual, was deemed sufficient for large banks and that the Reserve Bank could obtain appropriate information from other government organisations such as CERT NZ and NCSC.

Some respondents sought clarity on the expected level of details, such as the scope of our definition of "cyber events" (i.e. if it includes "acceptable use policies") or "cyber incidents" (i.e. if it includes phishing attempts, control failures and IT outages). There was also a clarification if it includes incidents outside of New Zealand for entities that operate in more than 1 jurisdiction.

The overarching concern of the entities is the cost of compliance as this requirement could entail reducing resources to focus on material cyber incidents to compile information on non-material cyber incidents. They noted that this could inflate the reporting of cyber incidents, which the entities have a comprehensive set of mitigating controls for, and will not help the Reserve Bank understand that the nature of cyber incidents impacting regulated entities. Some respondents added that collecting "low-level" type information does not appear to align with international data collection practices for cyber resilience.

Further on the details of the reporting requirement, some respondents requested for more information on the format of the reporting and greater clarity on our definition of "small entity" for the purposes of this proposed reporting requirement

To address the concerns raised, one suggestion is to make available to the Reserve Bank on request the potential material cyber incidents and material control weakness that did not meet the threshold for reporting. Some respondents also supported a narrower definition of "cyber incident" and some suggested that we obtain other relevant information from other government organisations such as the NSCC or CERT NZ that produce reports on local cyber security attacks.

Separately, a few respondents indicated that automated and continuous feed of cyber incidents might be more beneficial and more efficient to implement than periodic collection.

Reserve Bank's Response

We currently lack sector-wide data on trends on cyber incidents in the financial sector. This gap in information limits the Reserve Bank's understanding of the nature of the risk of cyber incidents impacting our regulated entities. The information currently available from other sources, such as the NCSC or CERT NZ, does not provide a holistic picture across all our regulated entities to provide insights for the sector to support our prudential functions.

We have considered the suggestion that we only collect material cyber incidents and not all cyber incidents. However, collecting only the incident data relating to material cyber incidents will provide an incomplete picture of the nature of cyber risk impacting the financial sector. A broader understanding of non-material cyber incidents, in particular the volume and nature of those incidents will provide a valuable understanding of the nature of cyber risk in the financial sector.

We have likewise carefully considered the comments on the level of detail in general. We note that as part of this requirement, our intention is to collect information on high level trends of volume by nature of cyber incidents. As such, we have developed a concise template for this requirement to ease compliance.

We have decided to maintain our proposed frequency of reporting (i.e. semi-annual for large entities and annual for all other entities). Receiving timely information is necessary in ensuring that

the policies in place remain fit-for-purpose. We also believe that the proposed reporting windows are feasible considering the requested information.

The definitions of "large entity," "small entity" and "cyber incident" in the material cyber incident reporting as discussed in the Reserve Bank's response to Q3 feedback are adopted in this reporting requirement. The reporting format is Excel as proposed and manual submission is expected until the online reporting system is put in place.

Cyber capability survey (Q5-Q6)

Q5: Do you have comments on our proposed cyber capability survey?

There were a range of views expressed on the value of the cyber capability survey. Majority of the submissions that explicitly expressed views on the relevance of the requirement were either supportive or not opposing it outright. Some respondents, however, questioned the appropriateness of the mechanism in obtaining information on the cyber resilience of an entity. Some also found the draft survey template to be too detailed and provides significant cyber intelligence on an entity while some opined that the proposed timeframe would be onerous for the reporting entities.

A respondent further mentioned that there is no response time provided apart from the suggested frequency of reporting. Other respondents also queried the appropriateness of the approach which does not distinguish entities based on their risk profiles (i.e. low, medium and high inherent risk).

Separately, some respondents wanted confirmation if the 2021 Guidance is a mandatory cyber resilience requirement, noting that it appears to be akin to a compliance review, while one submission sought for guidance on what "good" resilience means. Another respondent inquired whether the survey covers all systems in the organisation or only those relevant to New Zealand operations and customers. Meanwhile, some respondents sought for guidance on how large entities, which are expected to report annually, can respond to A1-Q4, A1-Q5, B2-Q5, B2-Q8, B3-Q4 and B3-Q6.

On the definitions of "small" and "large" entities, some respondents wanted clarity whether the NZD$2 billion threshold refers to assets or revenues and whether it includes agency partners in the context of insurance companies. In this regard, it was suggested that we use the concepts of Domestic Systemically Important Banks (D-SIBs) and non-D-SIBs to be consistent with how we categorise banks in other areas. There were also questions on the precise definitions of the supplied categorical responses "exceeds," "enhanced," "baseline" and "partial;" and the terms "relevant cyber training events/modules" (A3-Q11) and "security controls" (B2-Q4).

Given the differences in the capacities of reporting entities to comply with the proposed requirements, some respondents put forth options to consider as we proceed. These include having more flexible expectations on the responses; separate surveys for different reporting entity types or rewording the relevant questions to ensure relevance for both large and other entities; and independent assessment of the entity's capabilities against an industry-recognised framework, such as NIST Cybersecurity Framework.

Aligning our reporting requirement with the NIST Cybersecurity Framework (whose version 2.0 is currently being developed) and Cyber Risk Institute Cybersecurity Profile is mentioned to bring our requirement closer to the global standards.

On the delivery and collection of requested information, the respondents proposed that entities be given the option to provide information through direct engagement with the Reserve Bank instead of accomplishing the survey template. They also proposed that the Reserve Bank considers obtaining information from other government organisations that already collect them or collaborate with these agencies to reduce duplication; using anonymous online survey with higher level questions that provide data that can be aggregated at a sector level if the intent is to obtain a view of the sector's cyber resilience; and including cyber resilience in its regular prudential supervision with the entity.

Concerning the substance of the draft survey template, it was suggested that a requirement to provide an evaluation of the extent of systems coverage and successful restoration of critical system backups would be more effective in measuring an entities management of this risk as opposed to asking for the frequency of data logs (B3-Q4). It was also proposed to include a question about the readiness of incident response teams and executives to ensure that everyone is prepared in their roles in case major cyber incidents disrupt the institution.

Reserve Bank's Response

The cyber capability survey will be an important tool to understand the measures that regulated entities have instituted to deal with the evolving cyber risks. It will provide valuable information that will support our engagement with reporting entities on cyber resilience.

However, as with the material and periodic cyber incidents reporting, we acknowledge the comments on the template's level of detail. We agree that a number of the questions in the template could be rephrased to focus more closely on the qualitative alignment of the survey with our cyber resilience guidance.

In response to comments relating to the extent of information required, we have removed all the questions that ask for numeric responses (e.g., AQ4, AQ5, etc.), which substantially streamlines the reporting template. This will ease compliance and better focus the survey on self-assessment against aspects of the Reserve Bank's guidance.

For clarity, we split the question on the alignment of practices with the Reserve Bank's Guidance into two parts: (a) whether the entity has an existing plan/strategy/process and (b) whether this plan/strategy/process is in line with the Reserve Bank's Guidance (i.e. AQ7, AQ8 and AQ9). We provided reference notes where relevant and added a general comments section at the end to capture any additional comment or feedback (free text). Annex A3 summarises all the changes to the template that we sent out for consultation.

Regarding the response time, reporting will be on a regular cadence and entities will have the template available ahead of time. Individual entities will be able to manage how and when they choose to complete the survey as it suits them ahead of reporting deadlines.

We note that the 2021 Cyber Guidance (and any subsequent update of the document) is not designed to be a checklist for cyber resilience minimum requirements. Rather, entities are expected to design and develop their own cyber resilience framework that adequately addresses the specific cyber threats that they individually face. The guidance and frameworks developed by New Zealand's cybersecurity agencies (e.g. New Zealand Information Security Manual) and international organisations can be referred to if there is a need for more details. We assure the reporting entities, however, that we are always assessing the appropriateness of the policy approach.

We likewise emphasise that only systems in the organisation that are relevant to New Zealand operations are covered by the assessment.

In response to the questions on the frequency of reporting, we have made it clearer in the template that the assessment period is the prior 12 months for large entities and the prior 24 months for other entities, consistent with their respective reporting frequencies. The revised template also provides references that will help clarify the definitions of some of the key terms.

On our definition of large entities, we note that the NZD$2 billion threshold refers to total assets based on our proportionality framework and excludes agency partners in the context of insurance companies. Since the survey's coverage includes non-deposit taking institutions, definitions of Domestic Systemically Important Banks (D-SIBs) and non-D-SIBs would not be appropriate to use.

On the comments regarding the specific items in the draft survey, we acknowledge the value of having a requirement to provide an evaluation of the extent of systems coverage and successful restore of critical system backups to gauge risk management capacity, but this is beyond the information that we deem necessary. On the proposal to include a question about readiness of incident response teams and executives to disruptive cyber incidents, we believe that this is already captured by Section A1 of the template.

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

The majority of the respondents who expressed views on this question were comfortable with the proposed frequency of reporting if this becomes a requirement. One of the concurring respondents, however, emphasised the need to manage the timing of reporting and scale of reporting requests to ensure this requirement can be completed in a consistent and timely manner.

Separately, a respondent noted the rapidly growing list of regulatory requirements each year under a range of regulatory regimes. Thus, if this requirement were to be implemented, the respondent suggested that we consider a submission frequency of every 2 years for large institutions and every 3 years for other institutions. The respondent also suggested that we align the reporting with APRA's timetable to facilitate ease in compliance.

None of the respondents commented on the proposed thresholds to categorise reporting entities for this reporting requirement.

Reserve Bank's Response

We note the feedback received and we consider that every year for large entities and every 2 years for other entities are reasonable frequencies of reporting. As indicated in our response to the Q5 feedback, we have also narrowed the template to facilitate ease in compliance.

Information sharing, financial policy remit and policy prioritisation (Q7-Q9)

Q7: Do you have comments on how we propose to share information?

The respondents expressed broad support to share the information under the proposed reporting requirements. However, as underscored in their responses to the previous questions, they have concerns relating to data security. They requested for greater clarity on the information/data that will be shared, to whom they will be shared, and in what circumstances this would include

identifiable information. At least 1 respondent also queried if FMA will only receive Part A or Parts B and C as well of the material cyber incident reporting requirement.

Separately, guidance was sought on what the phrase "after considering the need to protect privacy and commercially sensitive elements of the information" means (page 16 of the consultation document). In relation to this point, several respondents pushed for safeguarding of data that can be linked with the entity's stakeholders, customers, partners, and employees in accordance with the Privacy Act 2020. The respondents further suggested that information, which identifies an entity, should not be shared without first notifying the entity that provided the information; and that the reporting entity should be given an opportunity to contest the sharing of non-anonymised information.

To mitigate the data security risk concern, some respondents reiterated their stance to anonymise and/or encrypt the data submitted. The view is driven by the perceived the risk of having extensive and potentially sensitive data concentrated within a single party if left unencrypted and un-anonymised, especially if it can be attributed to specific entities.

Several respondents also wanted more information on the measures that the Reserve Bank will take to store and protect the information submitted as well on the mechanism of sharing the learnings based on the data collected. Another suggestion in this regard was to only store the information for as long as it has an active purpose, otherwise it should be deleted.

Some respondents focused on data use protocols. Additional information is requested on (a) how each data point requested is aligned to the role of the Reserve Bank on receiving an incident report, (b) the purpose of collecting this information and (c) how this data will be used by the Reserve Bank. At least 1 submission indicated that it is not apparent from the proposals whether the Reserve Bank has the capacity/and capability to analyse all the information requested, and if so, how the ongoing provision of this information will contribute to its regulatory responsibilities and purpose.

Some respondents also queried whether regulated entities will be notified if data breaches happen to regulators holding the data submitted, including the Reserve Bank. In this regard, it was proposed to add a disclaimer which states that securing the channels to transmit data under the proposed reporting requirements remains a Reserve Bank accountability and that any "data-in-transit" and "data-in- storage" breaches would fall to the Reserve Bank for remedial action.

A related submission underscored the objective of ensuring that communications do not inadvertently cause public concerns about other financial institutions, assuring the public that any major breach issues are being managed system wide.

Reserve Bank's Response

We agree with the respondents on the importance of the ensuring the security and privacy of the data gathered in this exercise.

The Reserve Bank works to ensure that the design and implementation of any new technology capability has appropriate security controls in place to protect the data that we hold on behalf of our regulated entities. Our information systems additionally go through the Certification and Accreditation process and are assessed against the requirements of the New Zealand Information Security Manual. Security control requirements are determined based on the classification of the information stored, processed and/or transmitted by each system.

We will observe appropriate controls in sharing the information and information will only be shared if there is a proper purpose for doing so. The details of how the information sharing with other government agencies will be guided are still being developed. The collated information will likewise be anonymised and safeguarded following the Privacy Act 2020 and other relevant regulations.

As noted in our response to the Q3 feedback, we understand the efficiency issue of having to report to multiple agencies on the same incident. As such, we coordinate with FMA and other agencies to minimise reporting duplication. However, given the differences in mandates, reporting cannot be entirely confined to a single agency. We also have to safeguard certain information shared with us as part of our data privacy and security obligations. Thus, as mentioned, information sharing will be subject to appropriate security controls.

On the comments regarding the use of the information collected, as prudential regulator with a mandate to promote financial stability, it is critical for the Reserve Bank to have a sound understanding of the cyber risks that can substantially weaken the trust in our financial system. The information collected from regulated entities will help the Reserve Bank in supervising cyber risk impacting our regulated entities and incident response in the event of a cyber incident.

Q8: Do you have any comments on our analysis on the financial policy remit?

We received mixed views on this question. Those who agreed with the analysis appreciated the emphasis on proportionality, the greater cyber risk attached to larger financial institutions and the tiered approach to recognise that smaller entities have less resources than larger entities.

On the other hand, the respondents who disagreed with the analysis reiterated that the requirements would divert resources away from cyber resilience activities while unintended disclosure of sensitive information asked in the reporting requirements could increase cyber security risks. As such, they deemed that the regulatory and supervisory costs that come with the proposals are not proportionate to the expected benefits to the financial system and society. They also questioned the usefulness of the requested information, and the feasibility that the Reserve Bank will be able to review it all to obtain meaningful insights to enhance cyber resilience.

Some respondents sought clarity on the use of the phrase “low incidence of failure” in the first 2 relevant components of the financial policy remit that were cited in the consultation document. They posited that while it is stated that these components are not of high relevance, without adequate cyber resilience control processes and procedures, a "low incidence of failure" is not possible.

Some respondents likewise proposed to extend the application of proportionality to the details of the reporting requirement and timeframe for material cyber incident reporting.

Reserve Bank’s Response

As indicated in the consultation documents, we believe that the proposed data collection tools are crucial in obtaining timely information to guide our policies and foster financial market stability as cyber security risks evolve and become increasingly complex. However, we considered the points raised on ease in compliance. We also recognise the differences in capacity and risk profiles of regulated entities.

Given the abovementioned considerations, we have streamlined the templates as explained in our responses above. We have also provided reporting entities some flexibility in reporting material cyber incident updates and adjusted the frequency of reporting these updates. However, we have

decided to keep the timeframe for initial material cyber incident report, which we believe should be manageable regardless of size of the entity and taking into account the changes to the template. The proposed timeframes for the periodic reports notably already differentiate large from other entities.

In response to the comment on our analysis relating to the "low incidence of failure" component of the financial policy remit, we agree with the sentiment that cyber resilience is a relevant element to this component. Rather than classifying this component as not of high relevance, a more accurate classification may be that it is of some relevance, noting that there are a number of elements that may contribute to the potential failure of a regulated entity. We will update our analysis to reflect this point more accurately. However, while also important, the objectives of promoting financial inclusion, financial efficiency, and competition in the financial sector are not given as much weight in the context of this workstream.

Q9: Do you have comments on our proposed prioritisation of our cyber data collection proposals?

We received only 1 submission with an explicit view on the ordering of the reporting requirements and it agreed with our proposal. The views expressed in response to this question largely focused on the lead time that the entities would need to comply with the requirements. Some respondents indicated that unless there are changes to the templates, they do not deem it reasonable to implement the proposal as soon as possible this year.

They respondents contended that the reporting requirements will necessitate substantial work and a lead time of at least 6 months to satisfy on a regular and sustainable basis. They mentioned that the classified nature of the information that will require processes to be put in place to collate, encrypt and transfer the information in accordance with internal security and data protection policies.

Some respondents also wanted further discussions with the Reserve Bank in the form of open workshops where interested parties can raise questions and clarify parts of the proposals. At least 1 respondent suggested that consideration should be given to fast tracking next steps of entity assessments regarding governance. It emphasised the importance of ensuring that boards and senior management are appropriately aware of cyber resilience expectations as they should drive appropriate capability and a cyber-aware culture in their organisations, citing APRA's guidance (CPG 234, 2013) and mandatory standard (CPS 234, 2019) as bases.

Reserve Bank's Response

The implementation of the material cyber incident response requirement is our first priority. We have set the commencement date of the obligation on 8 April 2024. We have also taken on board feedback on timing of the two periodic surveys. The timeframes of these 2 reporting requirements are outlined in Table 1.

Table 1. Cyber resilience data collection key dates

Report	Obligation commencement date	First reporting due date
Material cyber incident reporting	8 April 2024	Ongoing

Report	Obligation commencement date	First reporting due date
Periodic cyber incident reporting	1 October 2024 (start of data collection)	30 April 2025 for large entities for the period from 1 October 2024 to 31 March 2025 (and every 6 months thereafter) 30 October 2025 for all other entities for the period from 1 October 2024 to 30 September 2025 (and annually thereafter) Submissions are due 30 days after the end of the reporting period
Periodic cyber capability survey	1 October 2024	1 October 2024 (and annually thereafter for large entities; biennially thereafter for all other entities)

Note: Large entities are defined as entities with at least NZD$2 billion in total assets following our proportionality framework.

Annex

The sections below detail the changes to the instructions and content material cyber incident template (see: red text). Items with changes to formatting and numbering are not included unless the corresponding text had also been changed. Items with changes that do not alter the substance of the questions/items are also not included (e.g. deletion of redundant words/phrases, grammar and spelling edits, etc.)

A1. Changes to the Material Cyber Incident Template Instructions

The Material Cyber Incident Notification Report consists of three parts:

- Part A - Initial Material Cyber Incident Report
- Part B - Material Cyber Incident Update
- Part C - Post Material Cyber Incident Conclusions

In the event you identify a material cyber incident, please report each part independently. You must provide regular updates to Part B as the material cyber incident advances. The only exception is where the material cyber incident is resolved within the 72 hours following identification, in which case if you complete Part A and the Conclusion section of Part C in full, you may submit these parts together without Part B.

Please answer the questions to the best of your knowledge at the time of completing this form, updates can be provided in future submissions as the cyber incident you are reporting on advances.

Be aware that during the notification reporting process RBNZ or FMA may request further information.

Survey: Please complete the Survey tab for each new submission of Parts A, B and C.

Sign-off: Please complete the Sign-off tab for each new submission of Parts A, B and C.

Part A. Initial Material Cyber Incident Report: Please complete the Part A tab as soon as possible when the material cyber incident is identified (no later than 72 hours after first identification). Please notify your supervisor that the material cyber incident notification report - Part A has been submitted.

Part B. Material Cyber Incident Update: Please complete the Part B Questions tab when any of the following occur:

- There have been developments in the incident impact or management or
- ~~It has been 24 hours since your previous submission of Part A or B, or~~
- You are requested to provide updates by your supervisor.

Note, you may need to revise and re-submit Part B numerous times depending on the nature of the cyber incident. Please notify your supervisor that the material cyber incident notification report - Part B has been submitted or re-submitted.

Additionally, note that completing Part B template in providing updates is optional. You can submit a similar report circulated internally provided that the information required is contained therein.

Part C. Post Material Cyber Incident Conclusions: Please complete the Part C Questions tab as a concluding full post-incident report as soon as practical, or when requested by your supervisor. Please notify your supervisor that the material cyber incident notification report - Part C has been submitted.

Cyber Incident Definition

A cyber event that:

~~i) jeopardises~~ adversely affects 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.

Material Cyber Incident Definition

A material cyber incident is ~~one which~~ an information security incident that 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 or other customers~~, system participants, or more broadly raises prudential concerns~~.

Detection Definition and 72-hour Reporting Window

Detection starts at the time when the materiality of the cyber incident has been established. The 72-hour timeframe pertains to calendar hours, which include non-business hours, public holidays and weekends.

Internal outage/service failure

Internal outage/service failure refers to an event that causes the system or service to be unavailable for use by any or all participants, regardless of: (a) the cause; and (b) the length of time of the outage.

Please refer to the FMA reporting section under the tab Survey if you are using this form to make a notification to the FMA

A2. Summary of changes to the Material Cyber Incident Notification Report Template[5]

Old Codes	New codes	Changes
C0.4.0	C0.4.0	If yes, ~~please~~ provide updates to the following questions C05.0 to C18.0 ~~before completing the Conclusion section~~. If no, ~~please~~ move on to Question ~~C23.0~~ C19.0, the Conclusion section. [Note: C19.0 refers to the new question code]

[5] Only questions items that have been changed/modified/deleted are included in the summary below. Mere changes to question codes due to changes in ordering of questions are not included.

Old Codes	New codes	Changes
B05.0-B05.5,	B05.0-B05.5,	For Questions B05.0 to B05.5, only enter fields where there has been an update/change since previous reporting.
C05.0-C05.5	C05.0-C05.5	For Questions C05.0 to C05.5, only enter fields where there has been an update/change since previous reporting.
A06.0		~~What is the current status of the incident? (please select one)~~ [Note: Deleted the entire item]
B06.0, C06.0	B06.0, C06.0	~~What is the current status of the incident? (please select one)~~ Has the severity classification of the incident changed since previous reporting? • Yes • No If yes, provide an update to the following question before moving to Question B07.0/C07.0. If no, move on to Question B08.0/C08.0. [Note: B07.0, C0.07, B08.0 and C0.8.0 refer to the new question codes]
A07.0	A07.0	What is the initial severity classification of the incident? (~~please~~ select one) • ~~Low~~ • Moderate • High • Severe RBNZ Comments ~~Low - A cyber incident which includes failed attacks, preliminary alerts, isolated targets, loss of non-critical systems or non-sensitive data for regulated entities, non-regulated entities, and other sectors.~~
~~A08.0-A09.0,~~ ~~B08.0-B09.0,~~ ~~C08.0-C09.0~~	A08.0, B08.0, C08.0	Which type of cyber incident (in A08.0) are you reporting on? (~~please~~ select ~~one~~ all that apply) [Note: Merged the 2 items into 1] RBNZ Comments Internal outage/service failure refers to an event that causes the system or service to be unavailable for use by any or all participants, regardless of: (a) the cause; and (b) the length of time of the outage.
	A08.5, B08.5, C08.5	Describe the affected system. (leave blank if not applicable)
~~A10.0~~	A09.0	How was the cyber incident you are reporting on detected? (select all that apply):

Old Codes	New codes	Changes
		• Internal controls • Outage notification (e.g. IT infrastructure, cloud) • Cyber attack detection notification • Cyber security ~~vulnerability alert~~ threat hunting or other security testing • Outsourced provider notification • Frontline staff/partners unavailability notification • Digital channels unavailability (e.g. website) • Customer notification • Staff compliance breach notification • Other
~~A11.0,~~ ~~B11.0,~~ ~~C11.0~~	A10.0, B10.0, C10.0	Customer ~~channel outage~~ impact
~~A11.1,~~ ~~B11.1,~~ ~~C11.1~~	A10.1, B10.1, C10.1	If you selected Customer ~~channel outage, please~~ impact (in A10.0), select which type of Customer channel outage. (select all that apply, leave blank if not applicable) • ATM • Branch/store network • Contact centre • Digital services (mobile) • Digital services (web) • Data loss • Other [Note: C10.0 refers to the new question code]
~~A14.3,~~ ~~B14.3,~~ ~~C14.3~~	A11.3, B11.3, C11.3	If possible, ~~please~~ estimate the total ~~size~~ number of ~~the customer impact~~ your clients (individuals and other entities) who were impacted. (select one)
~~A15.2,~~ ~~B15.2,~~ ~~C15.2~~	A12.2, B12.2, C12.2	~~Please d~~ Describe the impact on customer products. (leave blank if you selected none)
~~A15.3,~~ ~~B15.3,~~ ~~C15.3~~	A11.4, B11.4, C11.4	If possible, ~~please~~ estimate the percentage of your ~~entity's~~ total ~~customer base impacted~~ clients (individuals and other entities) who were impacted. (select one) [Note: Moved up]
~~A16.1,~~ ~~B16.1,~~ ~~C16.1~~	A13.1, B13.1, C13.1	Have any of these financial position and ~~market impact~~ operation categories been impacted by the incident you are reporting on? (select all that apply) • Trading activities • Transaction volumes and values • Monetary ~~losses~~ cost • Liquidity ~~impact~~ position • Withdrawal of funds • Other

Old Codes	New codes	Changes
		• None
~~A16.2,~~ ~~B16.2,~~ ~~C16.2~~	A13.2, B13.2, C13.2	Describe the impact on your financial positions and operations. (leave blank if no updates)
~~A18.0,~~ ~~B18.0,~~ ~~C18.0~~	A15.0, B15.0, C15.0	RBNZ Comment: Regulatory impact refers to impact on compliance with other regulations resulting from the incident.
~~A18.1,~~ ~~B18.1,~~ ~~C18.1~~	A15.1, B15.1, C15.1	If yes, describe the regulatory impact. (leave blank if not applicable)
~~B19.0,~~ ~~C19.0~~	B17.2, C17.2	~~Have there been additional actions taken to prevent further impacts to date?~~ What further actions have been taken to contain the impact/prevent further impacts? (exclude actions previously reported in this form) [Note: Merged with questions B21.0-B21.1, C21.0-C21.1 in the previous template; moved down]
~~A19.1,~~	A17.2	What actions have been taken to contain the impact/prevent further impacts to date? [Note: Merged with questions A21.0-A21.1 in the previous template; moved down]
~~B19.1, C19.1~~		~~If yes, please describe (leave blank if not applicable)~~ [Note: Deleted the entire item]
~~A20.0,~~ ~~B20.0,~~ ~~C20.0~~	A16.0, B16.0, C16.0	Who else has been notified about the incident? (select all that apply) • FMA • NCSC • CERT NZ • APRA • ASIC • OPC • Trustees (for NBDTs) • Other • None
~~A21.1,~~ ~~B21.1,~~ ~~C21.1~~	A17.1, B17.1, C17.1	~~If yes, please p~~ Provide a summary (leave blank if not applicable)
~~C22.0~~		~~Do you have an estimate of how long it will be until all interruptions to services have concluded?~~ [Note: Deleted the entire item]

Old Codes	New codes	Changes
~~A22.1, B22.1~~		If yes, when do you expect all interruptions to services ~~will~~ to conclude? ~~(please provide the date or the date and time, please leave blank if not applicable)~~
	A18.1, B18.1	Provide the date. (leave blank if not applicable)
	A18.2, B18.2	Provide the time. (leave blank if not applicable)
~~C22.1~~		~~If yes, when do you expect all interruptions to services will conclude~~ When did all interruptions to services conclude/when do you expect them to conclude? ~~(please provide the date or the date and time, please leave blank if not applicable)~~ RBNZ Comment: Conclusion of event/incident: The time when the incident has stopped occurring Interruptions to services: Services are unavailable to the users (Internal or external).
	C18.1	Provide the date. (leave blank if not applicable)
	C18.2	Provide the time. (leave blank if not applicable)
~~C23.0~~	C19.0	RBNZ Comment: Resolution of event/incident: The time when the root cause of the incident has been resolved.
~~C24.0~~	C20.0	RBNZ Comment: Recovery time: Amount of time for services to be available after an incident (based on the recovery time objective in ISO 22301); Refer to the Guidance on Cyber Resilience, page 21.
~~C31.0~~	C27.0	Which stakeholders have been informed or involved? • FMA • NCSC • CERT NZ • APRA • ASIC • OPC • Trustees (for NBDTs) • Other • None
		If no, do not complete questions C32.1 to C32.3.

Old Codes	New codes	Changes
	C32.1	If you answered yes to question C32.0, who is responsible for the review report??
~~C36.1~~	C32.2	If you answered yes to question C32.0, was this an independent review? [Note: C32.0 refers to the new question code]
~~C36.2~~	C32.3	If you answered yes to question C32.0, ~~there was a post-incident review report,~~ has a copy been submitted to your Primary Supervisor? [Note: C32.0 refers to the new question code]
		Part C general RBNZ comment: The respondent may repeat parts of their Post Incident Report to respond to the questions below.

A3. Cyber Capability Survey Cover Pages

We have added the following tabs in the revised template:

- Introduction page
- Sign-off page
- Instructions page

The survey respondents are expected to go over these tabs and provide the required information before submitting their accomplished survey questionnaire to the Reserve Bank.

A4. Changes to the Cyber Capability Survey Template

Code[6]	Questions	Data type	RBNZ Comments[7]
~~A.~~	A. Governance		
A1	A1. Board and Senior Management Responsibilities		
A1.Q1	~~Q1.~~ To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for governance responsibilities of the Board and Senior Management?	~~Exceeds/ Enhanced/ Baseline/Partial~~ Fully/Mostly/ Partially/Ad hoc	See Section A1 of the Cyber Guidance for definitions
A1.Q2	~~Q2.~~ Is there a dedicated Chief Information Security Officer or senior executive accountable for the cyber resilience strategy?	Yes/No	See Subsections A1.3, A1.3.1 and A1.3.2 of the Cyber Guidance
A1.Q3	~~Q3.~~ If yes, how long has the Chief Information Security Officer (or senior executive accountable	~~Numeric~~ Months/Years	

[6] The codes column has been added in the revised template.
[7] The RBNZ comments column has been added in the revised template.

Code[6]	Questions	Data type	RBNZ Comments[7]
	for the cyber resilience strategy) been in the role?		
	~~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~~	
A1.Q4	~~Q6.~~ Are internal audit results and incident "near misses" reported to the Board?	Yes/No	See Cyber Lexicon (p.17) for the definition of 'near miss.'
A2	A2. Cyber Resilience Strategy and Framework		
A2.Q1	Does your organisation have a Board approved cyber resilience strategy?	Yes/No/Ad hoc	See Subsections A2.1, A2.1.1 and A2.1.2 of the Cyber Guidance. Subsections A1.5 and A1.6 contain information on the responsibilities of the Board and senior management.
A2.Q2	~~Q7.~~ ~~Does~~ If yes, is your organisation's Board approved cyber resilience strategy ~~exist that is~~ consistent with the ~~Reserve Bank~~ Cyber Guidance?	Fully/Mostly/ Partially~~/Ad hoc~~	
A2.Q3	Does your organisation have a formally documented programme to maintain and increase your security posture and to deliver the cyber resilience strategy	Yes/No/Ad hoc	See Subsections A2.2-A2.6 of the Cyber Guidance.
A2.Q4	~~Q8.~~ If yes, is your organisation's ~~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~~ Cyber Guidance?	Fully/Mostly/ Partially~~/Ad hoc~~	
A2.Q5	Does your organisation have an internal audit process for your cyber resilience strategy and framework programme?	Yes/No/Ad hoc	See Subsection A2.5 of the Cyber Guidance.
A2.Q6	~~Q9.~~ ~~Do you have an~~ If yes, does your organisation's 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~~/Ad hoc~~	
A2.Q7	~~Q10.~~ How frequently is the cyber resilience strategy and framework programme reviewed ~~and updated~~?	Months/Years/Ad hoc	See Subsection A2.6 of the Cyber Guidance
A3	A3. Culture and Awareness		
A3.Q1	~~Q11. What percentage of staff completed the relevant cyber training events/ modules over the past 12 months?~~ Is there an organisation-wide regular (e.g. annual) cyber training programme?	~~Numeric~~ Yes/No	See Subsections A3.3, A3.3.1 and A3.3.2 of the Cyber Guidance. Subsection A1.4 is also relevant.

Code[6]	Questions	Data type	RBNZ Comments[7]
B	B. Capability Building		
B1	B1. Identify		
B1.Q1	~~Q1.~~ To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for capability building (Identify)?	Exceeds/ Enhanced/ Baseline/Partial	See Section B1 of the Cyber Guidance
B1.Q2	~~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/In progress	See Subsection B1.1 of the Cyber Guidance
	~~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~~	
B2	B2. Protect		
B2.Q1	~~Q1.~~To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for capability building (Protect)?	Exceeds/ Enhanced/ Baseline/Partial	See Section B2 of the Cyber Guidance and its subsections
	~~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~~	
B2.Q2	~~Q7.~~ Is a security assessment undertaken as part of change management?	Yes/No	See Subsections B2.5 and B2.6 of the Cyber Guidance
	~~Q8. How many times in the last 12 months have you assessed for cyber security risk (include data~~	~~Numeric~~	

Code[6]	Questions	Data type	RBNZ Comments[7]
	~~loss prevention, data egress checking, data classification)?~~		
B3	B3. Detect		
B3.Q1	~~Q1.~~ To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for capability building (Detect)?	Exceeds/ Baseline/Partial	See Section B3 of the Cyber Guidance and its subsections
B3.Q2	~~Q2.~~ Are anomalous activities and events being monitored and reported ~~on~~ to either the senior management or the Board?	Yes/No	See Subsection B3.1 of the Cyber Guidance
	~~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~~	
	~~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~~	
B3.Q3	~~Q8.~~ Were security tests also undertaken with all major changes in new systems or technologies?	Yes/No	See Subsection B3.7.1 of the Cyber Guidance
B4	B4. Respond and Recover		
B4.Q1	~~Q1.~~ To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for capability building ~~(Respond and Recover)~~?	Exceeds/ Enhanced/ Baseline/Partial	See Section B4 of the Cyber Guidance and its subsections
B4.Q2	~~Q2. Do you~~ Does your organisation have a response and recovery plan for ~~when a~~ cyber breaches ~~occurs~~ (in line with the recommendations of the ~~Reserve Bank~~ Cyber Guidance)?	Yes/No	See Subsection B4.1 of the Cyber Guidance
B4.Q3	~~Q3. If yes, when was the response and recovery plan last updated?~~ What is the frequency of review of the response and recovery plan?	Months/Years/Ad hoc	See Subsections B4.5, B4.6 and B4.7 of the Cyber Guidance
B4.Q4	~~Q4. Do you~~ Does your organisation use scenario testing (i.e. table-top exercise) to stress test your organisation's recovery plan?	Yes/No	See Subsection B4.5 of the Guidance

Code[6]	Questions	Data type	RBNZ Comments[7]
B4.Q5	~~Q5. Do you~~ Does your organisation have a process in place that incorporates lessons learned from cyber scenarios and incidents?	Yes/No	See Subsections B4.5 and B4.6 of the Cyber Guidance
B4.Q6	~~Q6. Do you~~ Does your organisation have a communications plan in place to notify external stakeholders of material cyber incidents?	Yes/No	See Section B4.8 of the Cyber Guidance and its subsections
B4.Q7	~~Q7. When was the communications plan last reviewed?~~ What is the frequency of review of the communications plan?	Months/Years/Ad hoc	
C	C. Information sharing		
C1	C1. Channels		
C1.Q1	~~Q1.~~ To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for information sharing channels?	Exceeds/ Baseline/Partial	See Section C1 of the Cyber Guidance and its subsections
C2	C2. Process		
C2.Q1	~~Q2. Is your organisation following the baseline recommendations in~~ To what level is your organisation following the ~~Reserve Bank~~ Cyber Guidance for information sharing process?	~~Fully/Mostly/ Partially~~ Exceeds/ Baseline/Partial	See Section C2 of the Cyber Guidance and its subsections
C2.Q2	~~Q3. Do you~~ Does your organisation have the capability to share anomalous activities and events detected?	Yes/No	Indicate Ad hoc if the processes followed are not based on established documentation; See Subsections C2.1 and C2.2 of the Cyber Guidance
D	D. Third-party management		
D1	To what level is your organisation following the Cyber Guidance for Third-Party Management for each of these categories?		
	~~Q1. Who are your third-party providers of critical functions and what services do they provide?~~	~~Please list.~~	
D1.Q1	~~Q2. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Planning~~)?~~	Exceeds/ ~~Enhanced/~~ Baseline/Partial	See Section D1 of the Cyber Guidance and its subsections
D1.Q2	~~Q3. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Due diligence~~)?~~	Exceeds/ Enhanced/ Baseline/Partial	See Section D2 of the Cyber Guidance and its subsections
D1.Q3	~~Q4. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Contract negotiation~~)?~~	Exceeds/ Enhanced/ Baseline/Partial	See Section D3 of the Cyber Guidance and its subsections

Code[6]	Questions	Data type	RBNZ Comments[7]
D1.Q4	~~Q5. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Ongoing cyber risk management~~)?~~	Exceeds/ Enhanced/ Baseline/Partial	See Section D4 of the Cyber Guidance and its subsections
D1.Q5	~~Q6. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Review and accountability~~)?~~	Exceeds/ Enhanced/ Baseline/Partial	See Section D5 of the Cyber Guidance and its subsections
D1.Q6	~~Q7. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Documentation~~)?~~	Exceeds/ Baseline/Partial	See Section D6 of the Cyber Guidance and its subsections
D1.Q7	~~Q8. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Termination~~)?~~	Exceeds/ Baseline/Partial	See Section D7 of the Cyber Guidance and its subsections
D1.Q8	~~Q9. To what level is your organisation following the Reserve Bank Guidance for Third-Party Management (~~Outsourcing to Cloud Service Providers~~)?~~	Exceeds/ Enhanced/ Baseline/Partial	See Section D8 of the Cyber Guidance and its subsections
	~~Part E: Resources~~	~~IT % of overall entity~~	
	~~E1. Total Organisation Headcount~~		
	~~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.~~ ~~Third Party IT providers~~ ~~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)~~ ~~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.~~		
E	General Comments: Provide any further comment (optional)		
E1	[Add any additional comments you think would aid us in understanding your organisation's cyber capability and resilience. If your comments	Free text	

Code[6]	Questions	Data type	RBNZ Comments[7]
	correspond with a specific question, indicate the question number.]		