RESERVE BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Guidance on reporting by banks of breaches of regulatory requirements

January 2021

Ref #9324601 v1.1

(1) Introduction

This guidance is intended to assist banks with their reporting obligations relating to the breach reporting and publication regime that came into effect from 1 January 2021. This regime applies to breaches of requirements set by any of the following instruments made under the Reserve Bank of New Zealand Act 1989 (the Act):

- A Condition of Registration (CoR) imposed under section 74;
- A notice requiring banks to have a credit rating issued under section 80; and
- An Order in Council made under section 81.

Under this regime banks are each subject to a notice issued under section 93 of the Act requiring them to report as soon as practicable when they become aware of information that leads them to form a belief (or ought to have led them to form a belief) that they have breached, may have breached, or may be likely to breach, one of the above requirements in a material respect. The Reserve Bank will then publish matters that it considers are actual material breaches of CoRs and section 80 notices on a dedicated page on its website.[1]

Banks are also required under the section 93 notices to provide six-monthly reports to the Reserve Bank of all matters they consider are breaches, whether material or not, in order to monitor whether they are correctly applying the threshold for material breaches.

All references to "breaches" in this document refer to matters that either the Reserve Bank or individual banks (rather than the courts) have concluded are or may be breaches.

(2) Bank becoming aware of breach

For the purpose of reporting that a bank has become aware of information leading it to consider that it has committed a breach (actual or potential), and for determining the date on which this has occurred, a bank is deemed to be aware once one or more directors or senior managers of the bank have actual knowledge of the facts which give rise to the need for disclosure. For this purpose, "senior manager" has the same meaning as in section 6(1) of the Financial Markets Conduct Act 2013.

(3) Reporting 'may have breached' or 'likely to breach' situations

Bank aware it may have breached a requirement.

A bank is deemed aware of information leading it to form the belief that it may have breached a requirement in the same way it is deemed aware of actual breaches. Reporting when a bank *may have breached* a requirement is intended to capture situations where the facts suggest that a specific breach may have occurred (or be occurring), but are not sufficient to form a view about whether it actually has occurred, or is occurring. Incomplete knowledge around the potential breach is not a reason to delay reporting the potential breach.

The information that must be reported on a 6-monthly basis does not include situations where a bank has identified in a 6-month period that it may have breached a requirement,

[1] The Reserve Bank will not publish potential breaches on its website (i.e. cases where a bank may have breached, or be likely to breach, a requirement), or apparent breaches that are not material. Material breaches of OiCs will also not be published on the Reserve Bank's website, as alternative arrangements are in place for dealing with breaches of those requirements (e.g. requiring disclosure statements to be republished with any necessary corrections).

and it was determined later in that same 6-month period that it has not actually breached that requirement.

Bank aware it is likely to breach a requirement

A bank is deemed aware it is likely to breach a requirement, as in section (1) above, in the same way it is deemed aware of actual breaches. The section 93 notices require immediate reporting to the Reserve Bank when a bank is aware it is likely to breach a requirement in a material manner. If the breach would not be material it should be included in the 6-monthly reports to the Reserve Bank.

The word *likely* is expected to be interpreted broadly, in line with its usual meaning. If a breach is expected, or considered probable, it should be reported under the 'likely to breach' criterion.

These considerations should be based on the facts available to the bank as it becomes aware of a specific potential breach. The reporting is not intended to capture events based on the general observation that future events are uncertain.

The bank may take into account any remedial action that it can take to reduce the likelihood of the potential breach. If the bank is confident that it can take action to fully remedy the problem or otherwise make the breach much less likely to occur, and expects to be able to do so before the earliest expected date of the breach, then the bank does not have to treat it as a likely breach.

Informal interaction with supervisors

None of these requirements are intended to delay or discourage early discussion of breaches, potential breaches or issues with the relevant Reserve Bank supervisor. Banks should continue timely and constructive engagement in accordance with the principles in the relationship charter.

(4) Materiality

The Reserve Bank considers that a form of "market-moving" test should provide a firm basis for what is of interest to investors visiting the breach-reporting webpage. However, the Reserve Bank also considers that there could be some types of breach that are not material for investors who are interested only in a bank's creditworthiness, but which raise material concerns about the bank from the perspective of the Reserve Bank as regulator. Examples may include a breach that is symptomatic of material control weaknesses even though it has not resulted in actual adverse outcomes, or a material breach of a policy designed to help resolvability after failure, such as the outsourcing and OBR policies. These categories of breaches should also be captured by the materiality threshold. In cases of doubt or borderline issues the reporting bank should err on the side of caution, reporting the breach as material.

High level tests

When a registered bank forms the belief (or ought to have formed the belief) that it has breached, may have breached, or is likely to breach a specified requirement, the bank should treat that actual or potential breach as material in any of the following cases:

1. If the bank considers that the Reserve Bank would regard the breach as raising prudential concerns.

2. In the case of a breach that has actually occurred, disclosure of that breach would materially affect the decision of a person to subscribe for debt securities of which the bank or any member of the bank's banking group is the issuer.

3. In the case of a breach that may have occurred or is likely to occur, if the breach had actually occurred disclosure of it would materially affect the decision of a person to subscribe for debt securities of which the bank or any member of the bank's banking group is the issuer.

It is expected that a reasonable number of breaches that occur will not qualify as material under the above tests. An example of a non-material breach would be an isolated incident of a minor nature that neither impairs the bank's ability to carry on business in a prudent manner, nor is of interest to investors or the wider public.

Materiality factors

In applying test 1 above ('raising prudential concerns') the following is a non-exhaustive list of factors that the Reserve Bank expects to be considered:

1. The impact of the breach on the bank's ability to carry on business in a prudent manner.[2]

2. The extent to which any matter in respect of the bank could result in financial consequences to the New Zealand financial system or to other banks.

3. The extent to which the breach had/has a negative impact on potential investors and depositors of the bank.

4. Whether the breach was negligent, reckless, or intentional.

5. The extent to which any matter may mislead or deceive the Reserve Bank.

6. The extent to which any matter could have a significant adverse impact on the bank's reputation.

7. How long the breach lasted (if already remedied), or is expected to continue.

8. Whether the breach is an isolated incident, or part of a recurring pattern of breaches in relation to a matter that is of the same nature.

9. The extent to which the breach or likely breach indicates that the bank's internal control and compliance frameworks to ensure compliance with the Conditions of Registration (CoRs) are inadequate.

10. The nature of the underlying CoR breached (whether it is narrow and objective, or a broader subjective requirement).

Examples

The following are examples of breaches that may be considered material:

- Credit exposures to connected persons that exceed the limits set in the Connected Exposures Policy.

[2] "The ability of the bank to carry on its business in a prudent matter" should be interpreted consistently with section s73(2)(c) and 78 of the Reserve Bank of New Zealand Act 1989.

- More than one-off or occasional lending above High-LVR restrictions.
- Running an unapproved internal model for capital adequacy calculations.

(5) Reserve Bank approach – materiality and consistency

It is the bank's own responsibility to take a view on materiality in the first instance. Banks are encouraged to engage with their Reserve Bank supervisor early when they consider that they have breached, may have breached, or are likely to breach a requirement. The Reserve Bank may take its own view on what is a material breach if necessary, and undertake supervisory action as it sees fit. Where the Reserve Bank concludes that a breach a bank has identified as not material is in fact material, it will provide that bank with the reasons for this conclusion.

The Reserve Bank will aim to promote consistency over time by using past decisions on when a breach was found to be material to inform its decisions on materiality in future cases. The Reserve Bank's view of a breach may change over time if more information becomes available.

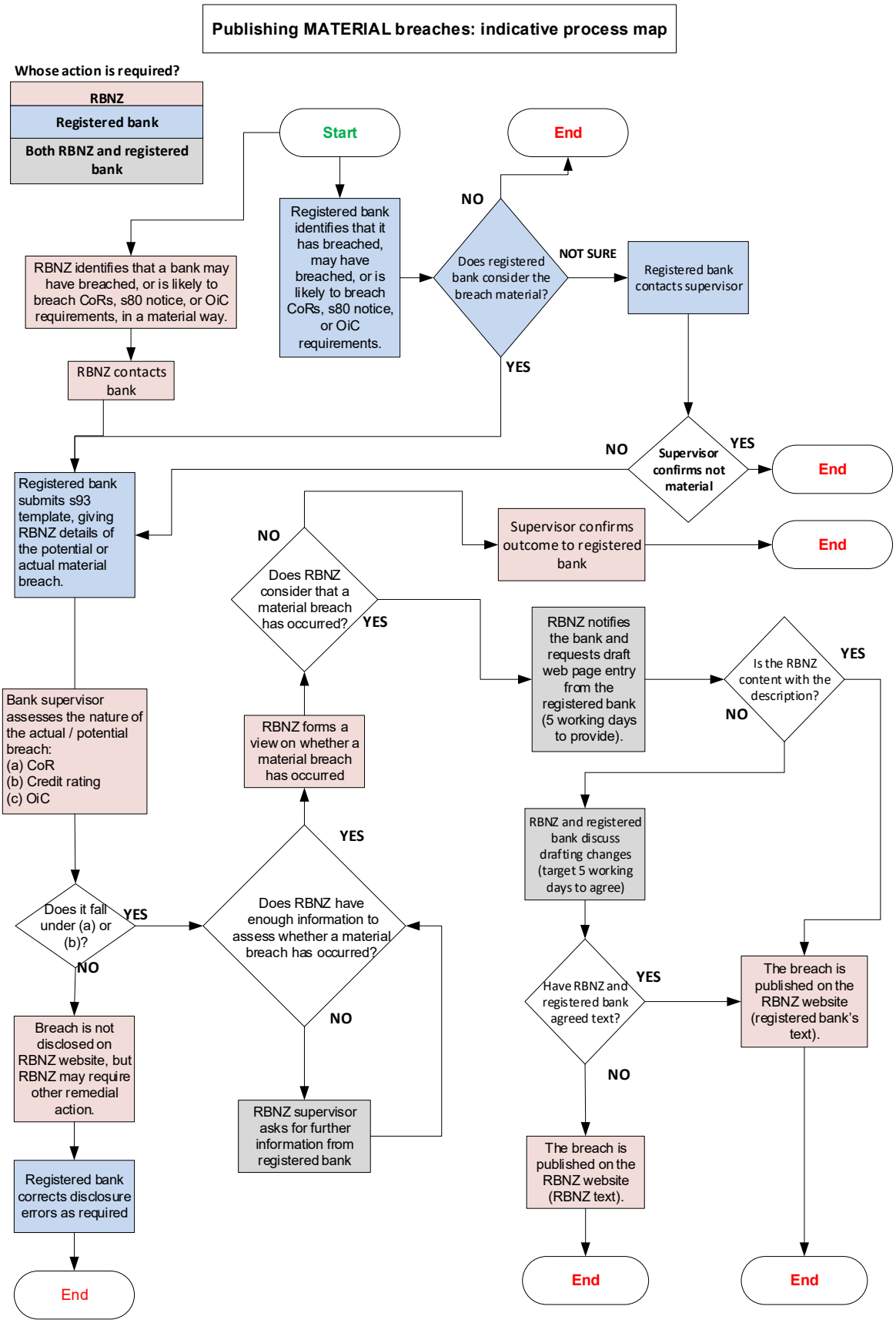
(6) Descriptions of breaches on the Reserve Bank website

Material breaches should be submitted to the Reserve Bank in the template provided with the section 93 notices.

In describing the nature and facts of the breach itself there is no pre-set word limit. However, the general approach is that the description should be adequate, should cover the facts, and should be long enough to do that but no longer.

The Reserve Bank intends to use, in general, relevant wording from the reporting entity's completed reporting template on the Reserve Bank's website. The process of publishing this information will involve a reporting bank having an opportunity to comment on the draft information to be published. The Reserve Bank retains final control of wording to be published on its website: in the rare event wording cannot be agreed with a reporting bank, the published breach will be accompanied by a note making clear the wording is not the reporting bank's wording.

When a breach has been fully remediated, the Reserve Bank will record this on its website.


Publishing MATERIAL breaches: indicative process map
Whose action is required?
RBNZ
Registered bank
Both RBNZ and registered bank
Start
End
RBNZ identifies that a bank may have breached, or is likely to breach CoRs, s80 notice, or OiC requirements, in a material way.
Registered bank identifies that it has breached, may have breached, or is likely to breach CoRs, s80 notice, or OiC requirements.
Does registered bank consider the breach material?
NO
NOT SURE
Registered bank contacts supervisor
RBNZ contacts bank
YES
Supervisor confirms not material
NO
YES
End
Registered bank submits s93 template, giving RBNZ details of the potential or actual material breach.
Supervisor confirms outcome to registered bank
End
NO
Does RBNZ consider that a material breach has occurred?
YES
RBNZ notifies the bank and requests draft web page entry from the registered bank (5 working days to provide).
Is the RBNZ content with the description?
YES
NO
Bank supervisor assesses the nature of the actual / potential breach:
(a) CoR
(b) Credit rating
(c) OiC
RBNZ forms a view on whether a material breach has occurred
RBNZ and registered bank discuss drafting changes (target 5 working days to agree)
YES
Does it fall under (a) or (b)?
YES
Does RBNZ have enough information to assess whether a material breach has occurred?
NO
Have RBNZ and registered bank agreed text?
YES
The breach is published on the RBNZ website (registered bank's text).
NO
Breach is not disclosed on RBNZ website, but RBNZ may require other remedial action.
RBNZ supervisor asks for further information from registered bank
The breach is published on the RBNZ website (RBNZ text).
Registered bank corrects disclosure errors as required
End
End
End