中國銀行
BANK OF CHINA

Bank of China US Branches
Key Risk Indicator Procedure

June 2021

Version	Date Changes Made	Author	Description of Changes
1.0	3/17/2017	Angela Lin; David Rush;	Established the first version
2.0	5/23/2017	Angela Lin; David Rush;	Update version
3.0	04/30/2018	Maggie Lai; Emily Zou	Annual update
4.0	10/23/2019	Maggie Lai; Emily Zou	Annual update
5.0	07/31/2020	Emily Zou; Agnes Liu	Annual update
6.0	06/03/2021	Agnes Liu	Annual update

Identifying Information	
Title	Bank of China US Branches Key Risk Indicator Procedure
Procedure Owner	ERM
Contact Information	Maggie Lai (blai@bocusa.com); erm@bocusa.com
Effective Date	xx/xx/2021
Location	https://bocus-sites/pub/policy/KRI Procedure (KRI procedure) K:\Public Folders\ERM\KRI Inventory (KRI Inventory)
Document Type	Procedure

Approved by	
Risk Management and Internal Control Committee	See 06/03/2021 RMICC Meeting Minutes

Reviewed by		
Yong Ma, EVP, Chief Risk Officer		
	Signature	Date
Maggie Lai, Head of ERM		
	Signature	Date

Contents

1. Executive Summary

Key Risk Indicators ("KRIs") are metrics used by Bank of China New York Branch and its satellite branches (collectively "BOC US Branches", "BOCNY" or "Branch") to monitor actual risk taking activities and provide early signal of increasing risk exposures across the eight risk areas of the Branch. They are quantitative metrics that indicate the quantity, direction and trend of a particular type of risk, providing BOCNY senior management and the US Risk and Management Committee ("USRMC") timely leading indicator information about emerging risks.

The Branch maintains two levels of KRIs. The first-level KRIs are the most critical branch-level aggregated KRIs contained in the Risk Appetite Statement ("RAS KRIs"). The second-level KRIs include other aggregated KRIs and department-level and business-line KRIs ("Non-RAS KRIs"). All KRIs are maintained in the BOCNY KRI Inventory.

This document, the Bank of China US Branches KRI Procedure ("Procedure"), establishes the governance protocols for managing KRIs and related reporting at both RAS and Non-RAS level according to the standards and risk management processes set up in the Bank of China US Branches Risk Governance Framework.

1.1. Rationale

The Procedure provides standard templates and reference materials to facilitate a consistent process for BOCNY Independent Risk Management ("IRM") and Front Line Units ("FLUs") to manage KRI lifecycle and conduct related reporting across the Branch.

1.2. Related Policies & Procedures

- Bank of China US Branches Risk Governance Framework ("RGF")

2. The Scope

This Procedure applies to FLUs and IRM departments and satellite branches of BOCNY as guidance in managing, monitoring and reporting of KRIs and risk-taking activities.

3. Roles & Responsibilities

3.1. Procedure Governance

Enterprise Risk Management Department ("ERM") is responsible for maintaining and updating the Procedure. The Procedure shall be reviewed by the Head of ERM and the Chief Risk Officer ("CRO"), and approved by the Risk Management and Internal Control Committee ("RMICC").

3.2. Procedure Implementation

This Procedure describes the governance protocol surrounding KRI change management, monitoring, reviewing, and reporting processes. The roles and responsibilities of relevant stakeholders are as follows:

USRMC: Responsible for approving the addition, modification, or removal of RAS KRIs as described further in *Section 4.2, RAS KRI*.

RMICC: Responsible for approving the addition, modification, or removal of RAS KRIs and Non-RAS KRIs as described further in *Section 4, Procedure Instructions*. For RAS KRIs, RMICC approval is prerequisite before submitting to the USRMC.

RMICC Subcommittees: Responsible for approving the addition, modification, or removal of relevant RAS KRIs and Non-RAS KRIs as described further in Section 4. RMICC Subcommittee approval is prerequisite before submitting to RMICC.

CRO: Responsible for proposing the addition, modification, or removal of RAS KRIs to the USRMC for approval. The CRO is also responsible for providing oversight of the overall KRI responsibilities laid out in this Procedure and ensuring the implementation of this Procedure.

FLUs and IRM: Responsible for implementing this Procedure as is further described in Section 4. IRM and FLUs are responsible for developing, monitoring, maintaining, modifying, reviewing and reporting KRIs. FLUs and IRM, as the KRI owner, should submit the KRI information to the relevant RMICC subcommittees and RMICC for review as appropriate. IRM and FLU specific responsibilities are differentiated for RAS KRIs and Non-RAS KRIs in Section 4.

ERM: Responsible for maintaining and updating this Procedure and providing related guidance. In addition, ERM is responsible for maintaining and managing the BOCNY KRI Inventory.

4. Procedure Instructions

The sections on procedure instructions provide detailed, step-by-step guidance on how to comply with the requirements that the Procedure intends to implement.

4.1. BOCNY KRI Inventory

The Branch's KRIs are tracked and maintained in the BOCNY KRI Inventory, which contains important information on both RAS and Non-RAS KRIs (e.g., KRI name, formula, risk type, description, ownership, etc.). If any BOCNY policy or procedure specifies the requirement of monitoring/reporting a KRI, that KRI is required to be included in the KRI Inventory. The KRI Inventory is maintained by ERM and can be found in: K:\Public Folders\ERM\KRI Inventory. KRI owners must submit the updated information to ERM after receiving appropriate approval from relevant committees. ERM is responsible for updating and maintaining the KRI Inventory at the Branch level after the KRI update has received appropriate approval from relevant committees.

4.2. RAS KRI

4.2.1. Roles and Responsibilities

USRMC: The USRMC is responsible for reviewing and approving RAS KRIs at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the Branch's business model, strategy, risk profile or market conditions. The USRMC is the final approval authority for RAS KRIs. Any addition, modification, or removal of KRIs in RAS shall be approved by the USRMC.

RMICC: Before any addition, modification, or removal of RAS KRIs is proposed to the USRMC, the RMICC shall approve the actions on RAS KRIs first.

RMICC Subcommittees: Before the IRM proposes any addition, modification, or removal of RAS KRIs to the RMICC, the relevant Subcommittee shall approve the actions on RAS KRIs first.

CRO: The CRO is responsible for proposing the addition, modification, or removal of RAS KRIs to the USRMC after RMICC approval.

IRM: IRM is responsible for proposing the addition, modification, or removal of RAS KRIs to RMICC and its subcommittees for approval. IRM is also responsible for submitting accurate RAS KRI information to ERM after USRMC approval to update the BOCNY KRI Inventory.

ERM: ERM is responsible for maintaining the RAS KRI Inventory and providing guidance regarding the RAS KRI governance protocols.

FLUs: Where applicable, FLUs can propose the addition, modification, or removal of RAS KRIs to the relevant IRM department and/or RMICC Subcommittees.

The table below summarizes the responsibilities of committees and departments.

	At USRMC	At RMICC	At RMICC Subcommittee	At Department
RAS KRIs	• Change Approval • Regular Reporting • Breach Reporting	• Change Approval • Regular Reporting • Breach Reporting	• Change Approval • Regular Reporting • Breach Reporting	• Monitoring

4.2.2. RAS KRI Addition, Modification, or Removal Process

The CRO, IRM and FLUs can propose changes to RAS KRIs. Changes proposed by FLUs must be endorsed by the relevant IRM areas. All changes to RAS KRIs must be presented by the IRM to the appropriate RMICC subcommittees and RMICC for approval, and then presented to the USRMC for final approval. The CRO is responsible for informing the Board of any major changes to the RAS KRIs as part of the approval process.

USRMC Directors can also propose changes to the RAS KRIs. The proposed changes should be discussed at the USRMC meeting.

Relevant information listed in the Information Required for KRI Update (See Section 7.1) should be provided when requesting committee approval.

4.2.2.1. Rationale for RAS KRI Changes

The rationale for the proposed changes should include an explanation of the need for the new or revised RAS KRI, the rationale to remove the KRI, the reasoning for the proposed new warning line and limit where applicable and the impact on the Branch's ability to manage risk. Where applicable, examples of the types of situations (e.g., change in risk profile, controls, or key processes) that the RAS KRI will help to monitor should be included as part of the rationale.

4.2.2.2. Guiding Principles for RAS KRI Creation and Limit Setting

The Branch follows a list of guiding principles to govern RAS KRI creation and warning line and limit setting. The major guiding principles for KRI creation include the following:

- Every KRI must be created with clear driver and specific purpose
- KRIs must be defined in a way to ensure clear understanding and accurate measurement
- Every KRI must have one department (i.e., KRI owner) that is ultimately responsible for monitoring and reporting the KRI
- An overall quality assurance process for each KRI must be established
- The creation and update of KRIs must go through appropriate governance process commensurate with its underlying risks
- All KRIs must be reviewed at least annually for potential updates to ensure effectiveness for relevant risk management

The major guiding principles for KRI limit setting include the following:

- Normally, every KRI should have a warning line and a limit
- Limits and warning lines for KRIs must be supported by strong rationale
- KRI owner must communicate with relevant departments regarding the proposed warning line and limit changes
- Newly defined and updated KRI warning line and limit must go through appropriate governance process commensurate with its underlying risks
- Warning lines and limits must be reviewed at least annually to ensure effectiveness for relevant risk management
- Warning line and limit breaches must trigger timely actions

4.2.2.3. Definition and Calculation Methodology

RAS KRI owners are responsible for providing a clear definition of RAS KRIs and the methodology used to calculate RAS KRIs. Such definition and methodology must be clearly documented in the BOCNY KRI Inventory. After USRMC approval, KRI owners should inform ERM in writing of the changes required in the BOCNY KRI Inventory, and ERM will make updates accordingly in the Inventory. RAS KRI owners must confirm that the data, calculation, and reporting processes used to monitor the RAS KRIs are reliable, appropriate for use, and properly documented.

4.2.2.4. Availability and Reliability of Underlying Data

An overall quality assurance process for each KRI must be established. KRI owners must work with data providers to perform data quality checks and confirm that data sources are:

- Available at the required frequency;
- Reliable in terms of quality; and
- Accessible to those performing the KRI calculation and monitoring.

KRI calculation should be automated using centralized data where possible. More data quality controls are needed for manually calculated KRIs.

A description of data controls and quality assurance processes used to ensure data accuracy should be made available by data providers upon request.

Any known data limitations, e.g., missing exposures or untimely data, should be documented and tracked centrally for resolution. Any known data limitations should also be communicated to the RAS KRI approval authority, i.e., RMICC and USRMC, and be noted on KRI reporting material.

4.2.2.5. Historic Trends and Current RAS KRI Status

Data providers of RAS KRIs must maintain data required to substantiate RAS KRIs. Historic information should be available if requested by IRM, Executive Management, or IAD. At minimum, data providers are required to maintain 3 years of historical data to calculate RAS KRIs. If the RAS KRI was created within 3 years of the reporting period then data providers are required to maintain data from the date the KRI was approved.

4.2.3. RAS KRI Review and Update Process

RAS KRI information should be reviewed and updated at least annually as part of the annual RGF review process.

- **Annual Update Process:** RAS KRI information is reviewed and approved at least annually as part of the RGF update requirements defined in the RGF (see RGF, Section 13.4). RAS KRI information is included in BOCNY KRI Inventory, which should be reviewed annually by relevant FLUs and IRM stakeholders. Where applicable, internal audit findings should be considered and addressed in FLUs and IRM review. ERM will define and publish the timeline and process before the annual review process. All departments need to review the relevant KRIs for potential updates to ensure effective risk monitoring, and attest the completion of RAS KRI annual review. RAS KRI owners should analyze whether the RAS KRIs and the associated limits are still appropriate and ensure all information for a RAS KRI documented in KRI Inventory is still correct.
- **Trigger Based Events and Off-Cycle Adjustments:** RAS KRIs may require off-cycle adjustments in response to internal or external developments. Events that may trigger an off-cycle RAS KRI adjustment include, but are not limited to:
  - Changes to the Branch's Strategic Plan;
  - Creation or retirement of products or business lines;
  - Changes to the Branch's risk profile or risk appetite;
  - Changes based on a determination that the underlying risk is better managed by a different KRI;

- Feedback from the USRMC, RMICC and/or its delegates, e.g., CEO or CRO;
- Feedback from IAD; and
- Emerging risks.

For the annual update process and off-cycle adjustments, the same roles and responsibilities for managing KRIs as laid out in Section 4.2.1 apply.

4.2.4. Communication and Awareness of RAS KRI Changes

Following USRMC's approval of the RAS KRI changes, e.g., addition, modification or removal of RAS KRIs, ERM must send the summarized updates via email to all departments.

4.2.5. RAS KRI Monitoring

The RAS KRI monitoring frequency is specified in BOCNY KRI Inventory. FLUs and IRMs are required to monitor the RAS KRIs and report to the relevant parties (e.g. relevant committees, CRO) if there is any adverse change in the trend.

4.2.6. RAS KRI Regular Reporting and Breach Reporting

There should be regular, accurate, and complete RAS KRI reporting and timely KRI breach reporting. This section outlines the protocol.

RAS KRI breach reporting thresholds are limits within which the Branch is intended to operate under the current risk tolerance level. Exceeding limits triggers breach reporting to the relevant committees. The process is discussed in *Section 4.2.6.2, RAS KRI Breach Reporting*.

4.2.6.1. RAS KRI Regular Reporting

4.2.6.1.1. Regular Reporting Frequency

IRM should submit KRI information to the RMICC and the USRMC quarterly. Additionally, IRM should report RAS KRIs to their respective RMICC Subcommittees according to the monitoring frequency documented in the KRI Inventory. All or part of the RAS KRI information may be requested for off-cycle reporting, e.g. for IAD/senior management review, regulatory requests, risk assessments or other reviews.

4.2.6.1.2. Roles and Responsibilities

RAS KRI owners, generally IRM, are responsible for the RAS KRI reporting processes. Regardless of where RAS KRIs are calculated, IRM is responsible for collecting and reporting RAS KRIs to the RMICC and the USRMC. In the case where a RAS KRI is owned by an FLU, relevant IRM and FLU can discuss and reach an agreement on the reporting process to RMICC and USRMC.

- **IRM (generally RAS KRI owners):** IRM is responsible for coordinating the establishment, monitoring, and reporting of KRIs in accordance with policies and procedures established by the various IRM functions. IRM is also responsible for (i) verifying the reasonableness of data

provided by FLUs, (ii) calculating KRIs assigned to IRM and (iii) reporting KRIs to the RMICC and the USRMC.

- **FLUs:** FLUs are responsible for ensuring that they operate within the established RAS KRI limits, and providing KRI data to IRM for Branch-wide aggregation and reporting to the RMICC and USRMC.

4.2.6.1.3. RAS KRI Reporting Data Gathering Process

In preparing the KRI information, the following data gathering procedures should be followed:

- ERM to provide the standard template for KRI reporting;
- IRM departments to update the template with KRI data for the risk areas they are responsible for; and
- IRM departments to submit their completed KRI information to ERM when available and per requested by ERM, whichever occurs earlier.

4.2.6.1.4. RAS KRI Source Data Quality Control

All identified data providers, IRM and/or FLUs, are responsible for ensuring that RAS KRI data are sourced and reported in accordance with the data governance and control standards specified in the RGF (see RGF, Section 10). The roles and responsibilities related to data quality are detailed in the data governance policies and related procedures established by CDO.

4.2.6.1.5. RAS KRI Regular Reporting Content

The KRI information is prepared by KRI owners and submitted to the RMICC and the USRMC quarterly. Regular reporting of RAS KRIs should include RAS KRI historical data and forecast data where applicable and/or available. Comments should also be included to explain KRI breaches if any and other important information that needs management and committee attention.

RAS KRIs with N/A as warning line and limit are created for monitoring purpose to ensure awareness from the Board and management. Given the nature of the metrics, it is not appropriate to define warning line and limit. KRI owners should report the actual value to corresponding RMICC subcommittee, RMICC and USRMC. If there is any major change of the actual KRI value, an in-depth analysis should be provided to the committees.

Upon request from KRI owners, data providers must provide supporting documents or information within a reasonable communicated timeline to give the KRI owners enough time to analyze the information for regular risk reporting.

4.2.6.2. RAS KRI Breach Reporting

Upon breaching the warning line of a RAS KRI, relevant parties should monitor closely, discuss the root cause, and evaluate its potential long-term impact. Close monitoring is required to prevent limit breach.

FLUs and IRM, in accordance with their respective responsibilities, should identify and report any breaches of the KRI limit.

In the case of a RAS KRI limit breach, the KRI owner should first notify its EVP-in-Charge, relevant department heads and ERM regarding the basic information of the breach within 2 business days after the breach is identified. Refer to Section 7.2 for relevant information required in the KRI breach notification. KRI owner will also need to provide evidence of the identification date to ERM.

Limit breaches must trigger timely actions. The KRI owner is also responsible for working with relevant IRM and FLUs to provide a written explanation of the breach. The written explanation, the KRI Limit Breach Escalation Memo, should be submitted to USRMC Secretariat in within 15 business days after the breach is identified. Relevant RMICC subcommittees and RMICC should also be notified. If the memo cannot be completed on time, KRI owners can submit request to CRO for exceptional approval of additional time. The rationale and a reasonable timeline should be provided in this process.

The following information should be provided in the KRI Limit Breach Escalation Memo (Section 7.3.1 RAS KRI Limit Breach Escalation Template):

- The cause of the breach;
- What actions, if any, are being planned to return to compliance, including who is responsible and a timeline for completion of such actions; and
- The risk concerns that the breach may have caused, including addressing the magnitude, frequency, and recurrence of breaches.

The memo should be prepared in both English and Chinese versions. The memo should be signed by the KRI owner, its EVP-in-Charge, other relevant departments and their EVP-in-charge as well as the CRO. The CEO should also be notified on the limit breach if the CRO deems necessary.

KRI owner department should drive the remediation action, and relevant departments responsible for breach remediation should follow the identified timeline to implement the actions accordingly. CRO and the EVP-in-Charge of KRI owner department and other relevant departments should oversee the remediation action. Relevant RMICC subcommittees, RMICC and USRMC should provide guidance on how to return to compliance as needed and appropriate.

In the case where a breach is anticipated to exist for a while, the KRI owner and relevant departments may request an exception to the breach reporting requirements stated above. The anticipated time period for this exception needs to be specified. An approval by the CRO, RMICC and USRMC is required for the exception.

4.3. Non-RAS KRI

4.3.1. Roles and Responsibilities

RMICC: The RMICC is responsible for reviewing and approving Non-RAS KRIs at least annually or more frequently, as necessary, based on the size and volatility of risks and any material changes in the Branch's business model, strategy, risk profile or market conditions. The RMICC is the final approval authority for Non-RAS KRI changes. Any addition, modification, or removal of KRIs in Non-RAS shall be approved by the RMICC.

RMICC Subcommittees: Before the IRM proposes any addition, modification, or removal of Non-RAS KRIs to the RMICC, the relevant subcommittee shall approve the changes on Non-RAS KRIs first.

IRM: IRM, if being the Non-RAS KRI owner, is responsible for proposing the addition, modification, or removal of Non-RAS KRIs and presenting the KRI changes to the appropriate RMICC subcommittees and RMICC for approval. For KRI changes proposed by FLU Non-RAS KRI owners, relevant IRM should provide review, challenge and guidance on the proposed changes as appropriate. IRM should support the FLU Non-RAS KRI owners to present the proposed KRI updates at RMICC subcommittees and RMICC.

ERM: ERM is responsible for maintaining the Non-RAS KRI Inventory and providing guidance to IRM and FLUs regarding the Non-RAS KRI governance protocols.

FLUs: FLU, if being the Non-RAS KRI owner, is responsible for proposing the addition, modification, or removal of Non-RAS KRIs as appropriate. FLU, as the KRI owner, should work with relevant IRM to present the KRI changes at RMICC subcommittees and RMICC.

The table below summarizes the responsibilities of committees and departments.

	At USRMC	At RMICC	At RMICC Subcommittee	At Department
Non-RAS KRIs	N/A	• Change Approval • Breach Reporting	• Change Approval • Regular Reporting • Breach Reporting	• Monitoring

4.3.2. Non-RAS KRI Addition, Modification, and Removal Process

Non-RAS KRIs provide FLUs with the ability to monitor day-to-day business activities and enable IRM to monitor risk indicators other than RAS KRIs.

FLUs and IRM departments can propose changes (addition, modification or removal) to the Non-RAS KRIs specific to their departments, business lines or risk area. Non-RAS KRI changes require endorsement by IRM (if proposed by FLUs) and approval by relevant RMICC subcommittee before submitting to RMICC for final approval.

Relevant information listed in the Information Required for KRI Update (See Section 7.1) should be provided when requesting committee approval.

4.3.2.1. Rationale for Non-RAS KRI changes

The rationale for the proposed change should include an explanation of the need for the new or revised Non-RAS KRI, the rationale to remove the KRI, the reasoning for the proposed new warning line and limit where applicable and the impact on the Branch's ability to manage risk. Where applicable, examples of the types of situations, e.g., change in risk profile, controls, or key processes that the Non-RAS KRI will help to monitor should be included as part of the rationale.

4.3.2.2. Guiding Principles for Non-RAS KRI Creation and Limit Setting

The guiding principles for the creation and limit setting for Non-RAS KRI are the same as the ones listed under Section 4.2.2.2.

4.3.2.3. Definition and Calculation Methodology

KRI owners are responsible for providing a clear definition of the Non-RAS KRI and the methodology used to calculate the Non-RAS KRI. Such definition and methodology must be clearly documented in the BOCNY KRI Inventory. Department heads or their designees of KRI owners must confirm that the data, calculation, and reporting processes used to monitor the Non-RAS KRIs are reliable, appropriate for use, and properly documented.

4.3.2.4. Availability and Reliability of Underlying Data

An overall quality assurance process for each KRI must be established. KRI owners must work with data providers to perform data quality checks and confirm that data sources are:

- Available at the required frequency;
- Reliable in terms of quality; and
- Accessible to those performing the KRI calculation and monitoring.

KRI calculation should be automated using centralized data where possible. More data quality controls are needed for manually calculated KRIs.

A description of data controls and quality assurance processes used to ensure data accuracy should be made available by data providers upon request.

Any known data limitations, e.g., missing exposures or untimely data, should be documented and tracked centrally for resolution. Any known data limitations should also be communicated to the approval authority, i.e., RMICC and relevant RMICC Subcommittees, and be noted on KRI reporting material.

4.3.2.5. Historic Trends and Current Non-RAS KRI Status

Data providers must maintain data required to substantiate Non-RAS KRIs. Historic information should be available if requested. At minimum, data providers are required to maintain 3 years of historical data to calculate Non-RAS KRIs. If the Non-RAS KRI was created within 3 years of the reporting period then data providers are required to maintain data from the date the Non-RAS KRI was approved.

4.3.3. Non-RAS KRI Review and Update Process

Non-RAS KRI information and BOCNY KRI Inventory should be reviewed and updated at least annually as part of the annual KRI Procedure review process.

- **Annual Update Process:** Non-RAS KRI information is reviewed at least annually by the relevant FLU and IRM stakeholders and approved by RMICC. Where applicable, internal audit findings should be considered and addressed in the review. ERM will define and publish the timeline and process before the annual review process. All departments need to review the relevant KRIs for potential updates to ensure effective risk monitoring, and attest the completion of Non-RAS KRI

annual review. Non-RAS KRI owners should analyze whether the KRIs and the associated limits are still appropriate and ensure all information for a KRI documented in KRI Inventory is still correct.

- **Trigger Based Events and Off-Cycle Adjustments:** Non-RAS KRIs may require off-cycle adjustments in response to internal or external developments. Events that may trigger an off-cycle adjustment include, but are not limited to:
  - Changes to the department / business line plan;
  - Creation or retirement of products or business lines;
  - Changes to the department or business line's risk profile or risk appetite;
  - Changes based on a determination that the underlying risk is better managed by a different KRI;
  - Feedback from the RMICC and/or its delegates, e.g., CRO and CEO;
  - Feedback from Internal Audit; and
  - Emerging risks.

For the annual update process and off-cycle adjustments, the roles and responsibilities as laid out in Section 4.3.1 apply.

4.3.4. Communication and Awareness of Non-RAS KRI Changes

Following RMICC's approval of the Non-RAS KRI changes, e.g., addition, modification or removal of Non-RAS KRIs, ERM must send the updated KRI information to relevant departments via email.

4.3.5. Non-RAS KRI Monitoring

The Non-RAS KRI monitoring frequency is specified in BOCNY KRI Inventory. FLUs and IRM are required to monitor the Non-RAS KRIs and report to relevant parties (e.g. relevant committees, department heads, IRM) if there is any adverse change in the trend.

4.3.6. Non-RAS KRI Regular Reporting and Breach Reporting

There should be regular, accurate and complete Non-RAS KRI reporting and timely breach reporting. This section outlines the protocol.

Breach reporting thresholds are limits within which the Branch/individual departments or business lines is intended to operate under the current risk tolerance level. Reaching limits triggers breach reporting to the relevant RMICC Subcommittees. The process is discussed in *Section 4.3.6.2, Non-RAS KRI Breach Reporting*.

4.3.6.1. Non-RAS KRI Regular Reporting

4.3.6.1.1. Regular Reporting Frequency

KRI owners should report Non-RAS KRIs to their respective RMICC Subcommittees according to the monitoring frequency documented in the KRI Inventory. All or part of the Non-RAS KRI information may

be requested for off-cycle reporting, e.g. for IAD/senior management review, regulatory requests, risk assessments or other reviews.

4.3.6.1.2. Roles and Responsibilities

KRI owners are responsible for the reporting processes. KRIs may be calculated by FLUs or IRM based on the availability of data, and other practical considerations. Regardless of where Non-RAS KRIs are calculated, KRI owners are responsible for collecting and reporting Non-RAS KRIs.

KRI owners are responsible for the establishment, monitoring, and reporting of KRIs in accordance with policies and procedures established by the various IRM functions. KRI owners are also responsible for (i) verifying the reasonableness of data contributed by data providers, (ii) calculating KRIs assigned to the owners and (iii) reporting Non-RAS KRIs to RMICC Subcommittees.

4.3.6.1.3. Non-RAS KRI Reporting Data Gathering Process

Data providers of Non-RAS KRIs are to provide data based on the requirements specified by Secretaries of RMICC Subcommittees.

4.3.6.1.4. Non-RAS KRI Source Data Quality Control

All identified data providers, IRM and/or FLUs are responsible for ensuring that Non-RAS KRI data are sourced and reported in accordance with the data governance and control standards specified in the RGF (see RGF, Section 10.2). The roles and responsibilities related to data quality are detailed in the data governance policies and related procedures established by CDO.

4.3.6.1.5. Non-RAS KRI Regular Reporting Content

The KRI information is prepared and reported to the RMICC Subcommittees by KRI owners. It should include historical data and forecast data when applicable and/or available. Comments on Non-RAS KRIs should be included to explain KRI breaches if any and other important information that needs subcommittee attention.

Non-RAS KRIs with N/A as warning line and limit are created for monitoring purpose to ensure awareness. Given the nature of the metrics, it is not appropriate to define warning line and limit. KRI owners should report the actual value to corresponding RMICC subcommittee. If there is any major change of the actual KRI value, an in-depth analysis should be provided to the committee.

Upon request from KRI owners, data providers must provide supporting documents, information, and/or data within 5 business days to give the KRI owners enough time to analyze the information for regular risk reporting.

4.3.6.2. Non-RAS KRI Breach Reporting

Upon breaching the warning line of a Non-RAS KRI, relevant parties should monitor closely, discuss the root cause, and evaluate its potential long-term impact. Close monitoring is required to prevent limit breach.

FLUs and IRM, in accordance with their respective responsibilities, should identify and report any breaches of the Non-RAS KRI limit.

In the case of a Non-RAS KRI limit breach, the KRI owner should first notify its EVP-in-Charge, relevant department heads and ERM regarding the basic information of the breach within 5 business days after the breach is identified. Refer to Section 7.2 for relevant information required in the KRI breach notification. KRI owner will also need to provide evidence of the identification date to ERM.

Limit breaches must trigger timely actions. The KRI owner is also responsible for working with the relevant IRM and FLUs to provide a written explanation of the breach. The written explanation, the KRI Limit Breach Escalation Memo, should be submitted to RMICC Secretariat within 20 business days after the breach is identified. Relevant RMICC subcommittees should also be notified. If the memo cannot be completed on time, KRI owners can submit request to CRO for exceptional approval of additional time. The rationale and a reasonable timeline should be provided in this process.

The information below covered by Non-RAS KRI Limit Breach Escalation Memo (Section 7.3.2 Non-RAS KRI Limit Breach Escalation Template) shall be provided to RMICC Subcommittees and RMICC:

- The cause of the breach;
- What actions, if any, are being planned to return to compliance, including who is responsible and a timeline for completion of such actions; and
- The risk concerns that the breach may have caused, including addressing the magnitude, frequency, and recurrence of breaches.

The memo should be signed by the department head(s) of the KRI owner and of the relevant departments.

KRI owner department should drive the remediation action, and relevant departments responsible for breach remediation should follow the identified timeline to implement the actions accordingly. Department head of the KRI owner and relevant department head(s) should oversee the remediation action. Relevant RMICC subcommittees and RMICC should provide guidance on how to return to compliance as needed and appropriate.
In case where a breach is anticipated to exist for a while, the KRI owner and relevant departments may request an exception to the breach reporting requirements stated above. The anticipated time period for this exception needs to be specified. In such situation, an approval by the RMICC is required.

5. Procedure Assurance Methods

5.1. Awareness Methods

The Procedure will be distributed to key stakeholders via email on an annual basis with key changes summarized. The Procedure is also available in the Policy Library.

5.2. Training Methods

ERM will provide training on this procedure and its application as needed or as the CRO determines is necessary to promote full understanding of the procedure.

5.3. Procedure Adherence Monitoring

ERM is responsible for monitoring and assessing the compliance with this procedure.

5.4. Update Requirements

This Procedure should be reviewed at least every three years or more frequently if necessary. Any changes to this procedure must be made by ERM and approved by RMICC.

5.5. Consequences of Violating the Procedure

Failure to comply with this Procedure will be escalated to the CRO and in certain circumstances to the RMICC, which will consider appropriate remediation action. Violations of the Procedure are grounds for disciplinary action based on the circumstances of the particular violation, the purpose of which action is to prevent violations and make clear that violations are neither tolerated nor condoned.

5.6. Exceptions & Exemptions

Exceptions to this Procedure should be considered case by case and be reported to CRO.

6. Reference Information

6.1. External Regulations

Below is a list of the applicable regulations. Please note that this list is not designed to be exhaustive or comprehensive.

- Office of the Comptroller of the Currency, *Large Bank Supervision: Comptroller's Handbook*, (Jan. 2010, Updated Dec. 2015)
- Office of the Comptroller of the Currency, *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations (Final Rule)*

6.2. Glossary

Abbreviation	Name
BOCNY	Bank of China New York
CDO	Chief Data Office
CEO	Chief Executive Officer
CRO	Chief Risk Officer

ERM	Enterprise Risk Management Department
FLU	Front Line Unit
IAD	Internal Audit Department
IRM	Independent Risk Management
KRI	Key Risk Indicator
RAS	Risk Appetite Statement
RGF	Risk Governance Framework
RMICC	Risk Management and Internal Control Committee
USRMC	US Risk and Management Committee

7. Appendix

7.1. Information Required for KRI Update

☐RAS KRI ☐Non-RAS KRI

☐KRI Addition ☐KRI Modification ☐KRI Removal

Required Information

- Addition:
  - Name of the KRI
  - Risk Type
  - Warning Line
  - Limit
  - Description (including Formula)
  - KRI Monitoring Frequency: [daily/monthly/quarterly, etc.]
  - KRI Reporting Frequency: [daily/monthly/quarterly, etc.]
  - Purpose for KRI Addition
  - Rationale for the warning line and limit setup, e.g., historical data/trend analysis with graphing, qualitative analysis, assumptions, etc.

- Modification:
  - Name of the KRI
  - Modification
  - Rationale for the modifications. For the update of warning line/limit, please provide the rationale for the limit setup, e.g., historical data/trend analysis with graphing, qualitative analysis, assumptions, etc.

- Removal
  - Name of the KRI
  - Rationale for why the KRI is no longer applicable

7.2. Information Required for KRI Breach Notification

- **Required Information**
  - Name of the KRI
  - Risk Type
  - KRI Owner
  - Warning Line
  - Limit
  - Breach Period
  - Actual Value
  - Breach Identification Date
    (To provide ERM with relevant evidence)
  - Next Step

7.3. KRI Breach Escalation Template

7.3.1. RAS KRI Limit Breach Escalation Template (English Version)

KRI Limit Breach Escalation Memo

To: **USRMC / RMICC / [RMICC Subcommittee]**

From: **BOCNY**

Breach Identification Date: **[Month Date, YYYY]**

Subject: **[KRI name] Risk Limit Breach in [Period, YYYY]**

Executive Summary
[PLACEHOLDER – Content]

Root Cause Analysis and Impact
[PLACEHOLDER – Content]

Observation by IRM (if applicable)
[PLACEHOLDER – Content]

Remediation Plan
[PLACEHOLDER – Content]

_____

Signature by Relevant Department Heads

_____

Signature by CRO and Relevant EVP(s)-in-Charge

7.3.2. RAS KRI Limit Breach Escalation Template (Chinese Version)

关键风险指标限额突破报告

收件人: **美国风险与管理委员会董事**

发件人: **中国银行纽约分行**

发现限额突破日期: **月份/日期/年份**

主题: **[限额突破出现年份/月份或季度] [关键风险限额指标名称] 限额突破报告**

概要
[具体内容]

根本原因及影响
[具体内容]

二道防线建议（如适用）
[具体内容]

整改/改进措施
[具体内容]

_____

相关部门总经理签字

_____

首席风险官及相关行领导签字

7.3.3. Non-RAS KRI Limit Breach Escalation Template

KRI Limit Breach Escalation Memo

To: **RMICC and [RMICC Subcommittee]**

From: **[Department name]**

Copy: **[Department name]**

Breach Identification Date: **Month Date, YYYY**

Subject: **[KRI name] Limit Breach in [Period/date, YYYY]**

Executive Summary
[Content]

Root Cause Analysis and Impact
[Content]

Observation by IRMs (if applicable)
[Content]

Remediation Plan
[Content]

_____

Signature by Department Heads of KRI Owner and Relevant Departments