Bank of China US Branches
Enterprise Risk Assessment Procedure
October 2020

Version	Date Changes Made	Author	Description of Changes
1.0	09/22/2016	Celia Yeh	Established first version of the procedure
2.0	10/18/2017	Emily Zou and David Rush	2017 Annual Update
3.0	07/01/2019	Marvin Chu and Tracey Huang	Updated for enhancements made to Enterprise Risk Assessment
4.0	10/20/2020	Tracey Huang and Yiwen Pan	2020 Annual Update

Identifying Information	
Title	Bank of China US Branches Enterprise Risk Assessment Procedure
Procedure Owner	Enterprise Risk Management Department
Effective Date	11/10/2020
Location	Policy Library
Document Type	Procedure

Approved by	
Risk Management and Internal Control Committee	See RMICC meeting minutes dated 11/10/2020

Table of Contents

1. Background

Bank of China New York Branch and its satellite branches (collectively "BOC US Branches", "BOCNY" or the "Branch") adheres to the Office of the Comptroller of the Currency's (OCC) guidelines establishing "Heightened Standards" that require:

- Front Line Units (FLU) to assess, on an ongoing basis, the material risks associated with their business activities
- Independent Risk Management (IRM) to oversee the Branch's risk-taking activities and assess risks and issues independent of FLUs

This document, the Bank of China US Branches Enterprise Risk Assessment Procedure ("Procedure"), establishes the process and guidelines for the Branch to conduct Enterprise Risk Assessments (ERA).

1.1. Rationale

This Procedure provides guidance to facilitate a consistent approach to perform enterprise risk assessments. Each FLU's self-assessment must provide analysis for applicable risk areas[1] within the FLU's scope of business activities and assess the FLU's effectiveness in managing each risk. IRM provides independent challenge to the self-assessments of each FLU as described herein and aggregates risk for each risk area and at the enterprise level. Internal Audit Department (IAD) provides independent review and challenge to the enterprise risk assessments prepared by FLUs and IRM through applicable audit activities.

1.2. Related Policies & Procedures

- Bank of China US Branches Risk Governance Framework

Bank of China US Branches Risk Governance Framework (the "RGF" or the "Framework") establishes the Branch's governance and risk management principles and standards, and has been developed in accordance with the OCC Heightened Standards (12 CFR part 30, Appendix D). This Procedure supports the RGF in identifying and assessing risks and issues.

2. Scope

This Procedure applies to all three lines of defense as guidance in execution and oversight of ERAs:

- FLUs: Business activities self-assessed (IRM and IAD excluded from self-assessment)
- IRM: Review and challenge of FLU self-assessments; provides final independent risk conclusion
- IAD: Independent review through applicable audit activities

[1] Risk areas established within the Branch's Risk Appetite Statement include compliance risk, credit risk, interest rate risk, liquidity risk, operational risk, price risk, reputation risk and strategic risk. Refer to *Appendix I: Determining Applicable Risks.*

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) periodically and approved by the Risk Management and Internal Control Committee (RMICC) whenever the Procedure is revised.

3.2. Procedure Implementation

Enterprise risk assessments described in this Procedure articulates the risk profile by FLU, risk stripe and at the enterprise level. The due diligence is supported by quantitative data and qualitative evaluation of the inherent risks, control effectiveness, residual risks and risk trends. The Branch performs enterprise risk assessments in order to identify current and emerging risks, assess their significance, determine trends, evaluate the Branch's risk appetite and identify areas of improvement to strengthen risk management activities. FLU self-assessments are evaluated by IRM in their independent assessment of the aggregate risk profile. Enterprise risk assessment results are considered by Executive Management for overall management of the Branch and as an input into the strategic planning process.

ERM has developed an assessment methodology, templates and a "Guidebook" to support the execution of enterprise risk assessments (Refer to *Appendix II: Enterprise Risk Assessment Template* and *Appendix III: Enterprise Risk Assessment Guidebook*). The reporting format captures risk rating and trend information for each risk stripe and may include rationale of changes in ratings or trends from the prior reporting period, if applicable.

Each of the three lines of defense has a role in the enterprise risk assessment process.

Front Line Units
Heads of FLUs are accountable for and must sign off on the FLU enterprise risk assessment results. FLU department heads may delegate this task to someone within his or her department. Prior to signing off on the results, FLUs must gather the relevant risk assessment information, perform the necessary analysis, evaluate the risks inherent within their business activities, evaluate the effectiveness of risk management and the control environment, conclude on the resulting level of residual risk, determine the risk trend and respond to any challenges and comments from IRM. FLU department heads are ultimately responsible for the substance of the FLU enterprise risk assessment and must be able to support and defend conclusions with the appropriate level of documentation. Where there are discrepancies at the departmental level between FLUs and IRM, the FLU is responsible for communicating the details of the discrepancy to the respective EVP in charge.

Independent Risk Management
The Chief Risk Officer and ERM determines the schedule for enterprise risk assessments with the objective to include the summary of the results as part of the risk management reporting materials to the US Risk and Management Committee (USRMC) and the RMICC.

IRM acts as a review and challenge function of FLU self-assessments. IRM reviews, provides a risk management perspective and independently challenges FLU self-assessments. IRM takes into account its independent view of inherent risks, control environment, economic and other external factors to evaluate the adequacy and accuracy of the self-assessments prepared by FLUs. Once the challenge session is complete, IRM summarizes the risk profile of each FLU and aggregates the risks into their respective risk stripe report.

ERM compiles enterprise risk assessments that reflect the aggregate risk across the Branch for all risk stripes, performs the final enterprise level aggregation and prepares the comprehensive Branch-wide enterprise risk assessment report.

Internal Audit Department

IAD evaluates the overall enterprise risk assessment process and reviews the enterprise risk assessments prepared by the FLUs and IRM as part of their periodic audits, ongoing monitoring, and its annual evaluation of the design and effectiveness of the RGF.

4. Procedure Instructions

4.1. Frequency of Enterprise Risk Assessments

The ERA is conducted on a quarterly basis. At the beginning of the calendar year, the "annual" ERA is conducted with a scope of the prior full calendar year. The annual ERA is the most comprehensive and establishes a "risk baseline" for the year. In the beginning of Q2, Q3 and Q4, the "quarterly" ERAs are initiated with a focus on identifying changes in the Branch's risk profile throughout the year by assessing prior quarter activities. A summary of the enterprise risk assessment results are included as part of the risk management reporting materials to the USRMC and RMICC. The CRO will discuss important risk profile changes with both committees and escalate any material risks to the USRMC.

4.2. Enterprise Risk Assessment Process

4.2.1. Enterprise Risk Assessment Preparation

On a periodic basis (and whenever there are significant changes in business activities), ERM works with IRM teams to confirm the following:

- Applicable inherent risk factors and weights to be assessed for the relevant FLUs
- Applicable control effectiveness factors and weights to be assessed for the relevant FLUs
- Weight of each FLU to the overall risk stripe rating including rationale

ERM works with the CRO to determine weight of each risk stripe to the overall enterprise level rating.

Training sessions are held with FLUs and IRM teams periodically. Feedback is obtained throughout the year and if applicable, incorporated into the templates and/or the Guidebook. To kick off each ERA process, ERM distributes the latest template (and Guidebook if there are updates) to the FLUs.

4.2.2. **FLU Enterprise Risk Assessment**

FLUs are responsible for completing the enterprise risk self-assessment utilizing the template and Guidebook to aid in the analysis. ERM has outlined the process for FLUs in the following seven steps:

Step 1: <u>Determine</u> which risks arise in your department
FLUs must determine which of the eight risks are applicable within their business activities. Refer to *Appendix I: Determining Applicable Risks* for a description of activities that give rise to each risk type. Note that central management of a risk type does not preclude a department from assessing the activity that give rise to that risk type.

If an FLU determines that a risk type is not applicable, a documented justification for its exclusion must be provided to ERM and await approval from the respective IRM team prior to being excluded from the ERA.

Step 2: <u>Gather</u> all relevant information
FLUs must consider all relevant information and documentation to conduct the enterprise risk assessment. Sources of information may include, but are not limited to:

- **Most recently published Key Risk Indicators (KRIs) and other applicable metrics**
  KRIs and other applicable metrics provide insight into the risk and controls environment as it relates to risk tolerances established within the Branch wide risk appetite. Indicators of risk levels should be considered in the context of the market environment and the complexity of business activities.

- **Current department strategic plan**
  The three year department level strategic plan documents key business and risk management initiatives. Enterprise risk assessment factors should be evaluated with these initiatives as inputs if applicable to the assessment period.

- **Output from other risk assessments and identification processes**
  Other risk assessments such as the Risk and Control Self-Assessment (RCSA) and any internal controls testing at the FLU or IRM level such as compliance testing, should be considered when assessing enterprise level risks and controls.

- **Any new products or services introduced since the prior enterprise risk assessment**
  If the FLU has offered a new product or service, the initial risk assessment from the new product approval process should be incorporated into the enterprise risk assessment. New products may increase the level of risk and as such, mitigating controls should be considered.

- **Results from audit activities and regulatory examinations**
  Results from audits and any applicable regulatory examinations should be considered and incorporated into the enterprise risk assessment. For example, any activities to address applicable audit findings should be considered when determining control effectiveness.

- **Information on geographic or market expansion**
  Any activities to expand market presence or move into a new market should be considered when assessing the inherent level of risk or risk trend. New markets and geographies that are foreign to the Branch may increase the level of risk.

- **Information on the external environment (e.g. competition, economy, regulatory environment)**
  If there is knowledge that the Branch's current markets have additional risk, such as softening real estate sales or an increase in unemployment, it should be incorporated into the inherent risk assessment. Also, changes in regulations or guidance that the Branch must comply with also presents additional risks.

Step 3: <u>Evaluate</u> inherent risk and control effectiveness factors
Once the FLU has determined which risk types are applicable and has gathered the relevant information, the enterprise risk self-assessment will be documented within the template contained in *Appendix II: Enterprise Risk Assessment Template*. The FLU self-assessment will rate inherent risk and control effectiveness factors, include supporting documentation (where applicable) and include a narrative to support the ratings. The factors in each risk area may have varying impact on the inherent risk or control effectiveness calculation. See section 4.2.4 below for details on the aggregation methodology.

Step 4: <u>Conclude</u> on the inherent risk and the control effectiveness
Once the FLU has performed the analysis and completed the self-assessment, the template will calculate a rating for inherent risk and control effectiveness for each risk stripe. Inherent risk rating will be either "low," "moderate," or "high." The control effectiveness rating will be either "strong, "satisfactory", "insufficient" or "weak." Risk rating definitions should be referenced when assigning ratings within the enterprise risk assessment template. Risk rating definitions can be found in *Appendix III: Enterprise Risk Assessment Guidebook.*

Step 5: <u>Determine</u> residual risk and risk trend
Determining Residual Risk
Residual risk considers both inherent risk and control effectiveness ratings. Guidance for determining residual risk is provided within the Guidebook, however, a formulaic approach may not always be appropriate. FLU has the option to "override" the rating recommendation in the Guidebook if there is a valid rationale. In addition to the factors being assessed, FLUs should apply judgement and business expertise in determining the level of residual risk.

Determining Risk Trend
FLU should consider whether risks are "increasing", "decreasing", or "stable" in the coming 12 months. This is determined by evaluating various sources of information (see Step 2 above). Similar to assessing any risk factor, the conclusion on risk trend should be supported by applicable documentation. After completion of the FLU self-assessment, FLUs sends the template to ERM to initiate the IRM review and challenge process.

Step 6: <u>Engage</u> in challenge sessions with IRM
Challenge sessions are a formal mechanism meant to provide IRM the opportunity to exercise professional skepticism with respect to the self-assessed ratings provided by FLUs. Challenge sessions may be in the form of in-person meetings, a phone call or through email exchange. IRM will reach out to FLUs regarding

additional clarification to ratings provided, to request additional documentation, to provide education on risk management standards, to confirm the understanding of business activities or to discuss differing viewpoints. If there are opposing views, the FLU and IRM should prepare an overview of facts supporting their respective viewpoints. Documentation of the review and challenge dialogue and outcome should be included within the template.

Step 7: Final Sign-off by FLU Department Heads

The final step for FLUs is for the department heads to sign off on the final enterprise risk assessment results documented within the template. If there are opposing views to the final rating of inherent risk, control effective, residual risk or risk trend, the FLU department head will need to communicate the discrepancy to their respective EVP in-charge as part of the sign off.

4.2.3. IRM Enterprise Risk Assessment

After the review and challenge session is complete, IRM will aggregate the results of all applicable FLUs and create an overall risk assessment report for each risk stripe. In this step IRM will rate the inherent risk factors, control effectiveness factors, residual risk and risk trend to form a conclusion at the aggregate risk stripe level. During this process, IRM will determine whether residual risks remain commensurate with the Risk Appetite Statement contained in the RGF. If supporting analysis indicates a residual level of risk that exceeds the qualitative goal of "low" or "moderate" in the Risk Appetite Statement, this must be clearly highlighted within the individual risk stripe report and IRM must assess efforts to address the discrepancy. ERM will then consolidate the eight IRM risk assessments and prepare an aggregate enterprise risk assessment report to summarize key risk areas. The enterprise risk assessment results and emerging risks considers both internal and external factors. The final ERA report is reviewed by the CRO and the summary of the results reported to both the RMICC and USRMC as part of the risk management reporting materials.

4.2.4. Enterprise Risk Assessment Aggregation

There are three levels of aggregation as part of the ERA process. The qualitative ratings are converted into a quantitative score, aggregated and converted back to qualitative ratings.

1. Qualitative Rating Conversion – Inherent Risk Factors, Control Effectiveness Factors, Residual Risk and Risk Trend

- Factors have been assessed using the following scale:

Inherent Risk	Control Effectiveness	Residual Risk	Risk Trend
Rating	Rating	Rating	Rating
High	Strong	High	Increasing
Moderate	Satisfactory	Moderate	Stable
Low	Insufficient	Low	Decreasing
	Weak		

- The qualitative ratings are the converted into a score using the following scale:

Inherent Risk		Control Effectiveness		Residual Risk		Risk Trend	
Rating	Score	Rating	Score	Rating	Score	Rating	Score
High	3	Strong	3	High	3	Increasing	3
Moderate	2	Satisfactory	2	Moderate	2	Stable	2
Low	1	Insufficient	1	Low	1	Decreasing	1
		Weak	0				

2. Three Levels of Aggregation – FLU, IRM and Enterprise Level

- For each in-scope FLU: Calculated by aggregating scores of relevant inherent risk, control effectiveness, residual risk and risk trend by the appropriate weight
- For each in-scope Risk Stripe: Calculated by aggregating scores of all in-scope FLUs by the appropriate weight
- For the aggregated Enterprise level results: Calculated by aggregating scores for all eight risk stripes by the appropriate weight

3. Quantitative Score Conversion – Inherent Risk Factors, Control Effectiveness Factors, Residual Risk and Risk Trend

- The quantitative ratings are the converted back into a qualitative rating using the following scale:

Inherent Risk		Control Effectiveness		Residual Risk		Risk Trend	
Score Range	Rating	Score Range	Rating	Score Range	Rating	Score Range	Rating
2.5<=score<=3	High	2.5<score<=3	Strong	2.5<=score<=3	High	2.5<=score<=3	Increasing
1.5<=score<2.5	Moderate	1.5<score<=2.5	Satisfactory	1.5<=score<2.5	Moderate	1.5<=score<2.5	Stable
1<=score<1.5	Low	0.5<score<=1.5	Insufficient	1<=score<1.5	Low	1<=score<1.5	Decreasing
		0<=score<=0.5	Weak				

4.3. Procedure Assurance Methods

4.3.1. Awareness Methods

The Procedure will be distributed to key stakeholders via email whenever there are updates with key changes summarized. The Procedure will also be available in the Branch's Policy Library.

4.3.2. Training Methods

ERM will provide training on this Procedure (or specific sections of the Procedure) periodically or as the CRO determines is necessary to promote full understanding of the procedure.

4.3.3. Procedure Adherence Monitoring

ERM is responsible for monitoring and assessing the compliance with this procedure. IAD evaluates the overall enterprise risk assessment process and reviews the enterprise risk assessment as part of their periodic department audits and annual evaluation of the design and effectiveness of the RGF.

5. Update Requirements

ERM is responsible for taking a proactive role to ensure that this Procedure remains relevant and comprehensive. ERM should review the Procedure at least annually and make updates at least every three (3) years or more frequently if needed.

5.1. 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 activities. Violations of the Procedure are grounds for disciplinary action, adapted to the circumstances of the particular violation as violations are neither tolerated nor condoned.

6. Exceptions & Exemptions

There are no exceptions or exemptions to this Procedure.

7. Reference Information

7.1. 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*
- 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)*

8. Glossary

Acronym	Definition
BOCNY	Bank of China New York
CRO	Chief Risk Officer
ERA	Enterprise Risk Assessment
ERM	Enterprise Risk Management Department
FLU	Front Line Unit
IAD	Internal Audit Department
IRM	Independent Risk Management
KRI	Key Risk Indicator
OCC	Office of the Comptroller of the Currency
RCSA	Risk and Control Self-Assessment
RGF	Bank of China US Branches Risk Governance Framework
RMICC	Risk Management and Internal Control Committee
USRMC	US Risk and Management Committee

9. Appendix

9.1. Appendix I: Determining Applicable Risks

Compliance Risk
Compliance risk is not limited to risk from failure to comply with BSA/AML, OFAC Sanctions, Bank Regulatory, and consumer protection laws. It encompasses the risk of noncompliance with all applicable laws and regulations, as well as prudent ethical standards and contractual obligations. It also includes the exposure to litigation (known as legal risk) from all aspects of banking, traditional and nontraditional. All FLUs must assess compliance risk associated with their activities.

Credit Risk
Credit risk arises in all activities in which settlement or repayment depends on counterparty, issuer, or borrower performance. Credit risk exists any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet. All businesses that engage in lending activity, investment activity, or settlement activities should assess credit risk.

Interest Rate Risk
Interest rate risk results from: differences between the timing of interest rate changes and the timing of cash flows (repricing risk); changing interest rate relationships among different yield curves affecting bank activities (basis risk); changing interest rate relationships across the spectrum of maturities (yield curve risk); and interest-related options embedded in bank products (options risk). Businesses where lending or investment activities take place must consider the level of interest rate risk posed by deal pricing and structure within risk assessments.

Liquidity Risk
Liquidity risk includes the inability to access funding sources or manage fluctuations in funding levels. Any business that requires funding to create assets naturally gives rise to liquidity risk. As such, all lending, investment, and some settlement activities should be considered when assessing liquidity risk.

Operational Risk
Operational losses result from: internal or external fraud; inadequate or inappropriate employment practices and workplace safety; failure to meet professional obligations involving clients, products and business practices; damage to physical assets; business disruption and systems failures; and failures in execution, delivery and process management. All FLUs must assess operational risk associated with their activities.

Price Risk
This risk occurs most significantly from market-making, dealing, and position-taking in interest rate, foreign exchange, equity, commodities and credit markets. Settlement activities involving currency conversion also give rise to price risk. Any business that engages in these activities must assess price risk as it relates to its activities.

Reputation Risk
Reputation risk is inherent in all Branch activities and requires management to exercise caution when interacting with stakeholders, such as customers, counterparties, correspondents, investors, regulators, employees and the community. The assessment of reputation risk should take into account the Branch's culture, nature of business activities and mechanisms to identify reputation events. All FLUs should assess the reputation risk associated with their activities.

Strategic Risk
The assessment of strategic risk includes more than an analysis of a Branch's written strategic plan. It focuses on opportunity cost and how plans, systems and execution activities affect the FLUs and the Branch's financial condition and resiliency. It also incorporates management's analysis of external factors such as economic, technological, competitive, regulatory and other environmental changes that affect the bank's strategic direction. All FLUs must assess the strategic risk associated with their activities.

9.2. Appendix II: Enterprise Risk Assessment Template

Enterprise risk assessment templates have been created for each risk stripe and are customized based on the nature of business activities performed by each FLU. Enterprise risk assessment templates can be found in the shared drive (K:\Limited Authorized Access Folders\ERM\Enterprise Risk Assessment\New ERA Process).

9.3. Appendix III: Enterprise Risk Assessment Guidebook

The Enterprise Risk Assessment Guidebook has been developed to support the execution of the enterprise risk assessment. Feedback is obtained throughout the year and if applicable, incorporated into the Guidebook. The latest Guidebook is distributed to the FLUs to kick off each ERA process and can be found in the shared drive (K:\Limited Authorized Access Folders\ERM\Enterprise Risk Assessment\New ERA Process).