I. Purpose Statement

The purpose of this document is to define what a risk assessment is and how the Information and Cyber Risk Management ("**ICRM**") team performs them.

II. Approach

- By utilizing an inventory of applications, infrastructure components, vendor-hosted applications and cloud offerings, **ICRM** determines the **inherent risk** rating of each of the aforementioned items within the inventory by conducting a **BIA**. This will then determine which items requires an **ICRA**, the frequency they are to occur and which items require independent/third party assessment and/or validation.
  - To determine the **inherent risk** rating, the **BIA** takes into consideration: business impact, regulatory requirements, related infrastructure components and third-party service providers' ("TPSP") Tier (*i.e.*, TPSPs from Tier 1 through to Tier 3).
  - Additional examples of items of consideration include:
    - Recovery Time Objectives ("RTOs");
    - Recovery Point Objectives ("RPOs");
    - Regulatory (*e.g.*, FDIC, GLBA, NYDFS Part 500);
    - Confidential or Restricted data is processed, stored or transmitted;
    - Volume of records present within a particular system;
    - Criticality of an asset as per the Risk Management Materiality Framework
  - The triggers, which determine whether an **ICRA** must be conducted, includes, but is not limited to the following: new application deployment, network changes, major changes to existing application/infrastructure components, or after the completion of a significant IT project (prior to deployment into the Production environment).
  - The **inherent risk rating** determines the frequency in which an ICRA must be conducted:

Inherent Risk Rating	ICRA Frequency	Independent Testing
Very High	Annual	Yes
High	Annual	Yes
Moderate	Once every 2 years	Yes
Low	Once every 2 years	No

- The next stage of the **ICRA** is the **TVCA**: During this stage, **ICRM** schedules and conducts workshop sessions with the various Line-of-Business ("LoB") Owners/Department Heads as well as the Business Owners and Application Owners during which ICRM team members complete a questionnaire. After the questionnaire is complete with issues identified, ICRM sends out a Request List. The purpose of the Request List is to collect artifacts and other evidence to perform Validation of the questionnaire. ICRM examines the artifacts and evidence to determine the adequacy of controls and generates a **control rating**.
- An issue (typically a control gap) noted by **ICRM** during the **TVCA** portion of the **ICRA** is examined and the **inherent risk rating** and **control rating** are considered and there is a determination of the **residual risk**. If an issue has a **residual risk** rating that exceeds the Bank's risk appetite, it is then considered a **Finding** (which warrants an overall assignment of criticality and an agreed upon remediation/corrective action plan with both the Issue Owner and Remediation Date identified).

  [See *Figure 1*]
- **Findings** are expected to be resolved/remediated within this time frame:

	Very High/High	Moderate	Low
Timeframe	3 months	6 months	12 months

- Issues and remediation actions identified by ICRM should be loaded into the Bank's GRC tool. Material issues and actions, along with status, should be reviewed at the Information Security Sub-Committee. If the action plan is not completed by the due date, the issue will be reported to the MRC. Information Security should review the closing support documentation for material issues and actions prior to closing in the GRC tool.

III. Glossary

Information and Cyber Risk Assessment ("ICRA") – A large-scale, deep-dive risk assessment performed on a particular information resource.

Business Impact / Criticality Assessment ("BIA") – A component of the ICRA detailing the criticality of the information resource to the Bank by the documentation of potential loss events and the business impact for when confidentiality, integrity, and/or availability of the information resource or the data contain within has been compromised. The results of this assessment forms the basis of the **inherent risk** rating.

Threats, Vulnerability, and Control Assessment ("TVCA") – A component of the **ICRA**; captures the threats and vulnerabilities related to the information resource under assessment; identification of the controls in place and other factors which mitigate or reduce the likelihood and impact of those threats and vulnerabilities if exploited. The results of this assessment forms the basis of the **control rating**.

Finding – An issue noted by **ICRM** during the **ICRA** process; typically a control gap or weakness that, left unaddressed, results in a **residual risk** rating that exceeds the bank's risk appetite; warrants an assignment of criticality (Very High, High, Moderate or Low) and an agreed upon remediation/corrective action plan with both the Issue Owner and Remediation Date identified:

Figure 1

IV. Assumptions

- All information assets, infrastructure components, vendor-hosted applications and other related-resources, *etc.* have all been entered into the appropriate inventory system;
- Both the Business Owner and Application Admin (*e.g.*, an IT owner) have been identified for each information asset

Standard Author:

Joseph Martano

AVP, Cyber Risk Analyst

Jonathan Ruf

VP, Information Security

Standard Approved By:

Max Tumarinson

SVP, Chief Information Security Officer ("CISO")

Appendix

Risk Management Materiality Framework

Materiality Framework During Normal Situations

	Frequency		Financial Impact		
	Possible / Adverse Stress	Probable / Baseline Conditions	Profit and Loss Impact	Core Equity Impact (CET-1)	Balance Sheet Impact
Frequency Definition:	Event may occur over a business cycle (e.g. within 5~10 years)	Event occurs in business-as-usual situations (e.g. every year)			
Impact	VH	VH	>$5mm (~5% Earnings)	>50 bps	>5%
	H	H	$2mm - $5mm	20 bps - 50 bps	2% - 5%
	M	M	$1mm - $2mm	10 bps - 20 bps	1% - 2%
	L	L	<$1mm	<10 bps	<1%

	Frequency		Non-Financial Impact		
	Possible / Adverse Stress	Probable / Baseline Conditions	Regulatory Impact	Customer Impact	Reputational Impact
Impact	VH	VH	Significant regulatory scrutiny; potential loss of business license; significant fines	Significant impact / loss of customers; likely litigation / compensation claims; significant loss of deposits	Trustee impact, deterioriation of Bank owner's value
	H	H	Regulatory scrutiny; possible legal action/regulatory fines; likely to result in improvement order	Potential financial detriment to customers / loss of customers	Negative media coverage in general public
	M	M	Internal compliance issues; possibly reportable to regulator; could result in improvement order	Moderate impact to customers, limited to a relatively small number	Negative coverage within industry
	L	L	Disciplinary warning; minimal regulator action	Minimal potential for customers impact	Negative press unlikely

Materiality Framework During Exceptional Situations				
	Frequency	**Financial Impact**		
	Remote / Severe Stress	Profit and Loss Impact	Core Equity Impact (CET-1)	Balance Sheet Impact
Frequency Definition:	Event occurs in exceptional situations (e.g. tail risk, beyond 10 years)			
Impact	VH	>$10mm (~10% Earnings)	>100 bps	>10%
	H	$4mm - $10mm	40 bps - 100 bps	4% - 10%
	M	$2mm - $4mm	20 bps - 40 bps	2% - 4%
	L	<$2mm	<20 bps	<2%