2023 FIRMA National Risk Management Training Conference

May 2, 2023

San Antonio, Texas

Risk Assessments - Beyond the Basics

Joan Dindoffer - 1st Line

Carol Severyn - 2nd Line

Natalie McCabe - 3rd Line

Stephen Cantrell - 3rd Line

Note: Views expressed are those of the respective speakers and not necessarily those of FIRMA or any particular institution except as indicated, and do not constitute legal advice.

Three Lines of Defense

- First Line: Front Line Units / Business Units
- Second Line: Independent Risk Management (IRM)
- Third Line: Audit

EACH HAS A DISTINCT BUT COMPLEMENTARY ROLE

No “One Size Fits All”

A Risk Management Program should be:

- Appropriately tailored to an organization’s risk profile
- In complex organizations, expect a firm-wide approach with ties to the Bank’s Risk Appetite Statement, Risk Governance Framework, and parameters set in those documents
- In smaller, less complex institutions, a less centralized program may be seen
- OCC and Fed have established heightened standards for >$50B banks
- Purpose - to identify, assess, control, measure, monitor, & report risks

Refer to Standards Set Forth in:

- OCC Comptrollers Handbook, Corporate and Risk Governance, 7/2019
- OCC “Bank Supervision Process” booklet of Comptroller’s Handbook, 6/2018
- Federal Reserve SR 08-8, Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles, revised 2/26/2021
- 12 CFR 30, Appendix D, OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured National Banks, Insured Federal Savings Associations, & Insured Federal Banks

Front Line Units

First Line of Defense

First Line

Policies: High level statements so that front line risk is:

- Identified
- Measured
- Monitored
- Controlled
- Consistent with Bank's Risk Appetite Statement and within Risk Governance Framework

Procedures: Build out processes to comply with policies

First Line

SAMPLE POLICY

Policy: Trust Compliance Program

The Trust Division will support the enterprise's Risk Appetite Statement as the aggregate level of risk that the enterprise is willing to assume to achieve its strategic objectives from a quantitative and qualitative perspective. It recognizes the enterprise risk across the following risk pillars, as applicable, and as they may be adjusted from time to time: Credit, Interest Rate, Liquidity, Price, Operational, Compliance, Strategic, and Reputational.

The Trust Division recognizes that the enterprise's objective, and the Division's objective is not to eliminate risk, but rather, to understand, manage, and appropriately consider those risks. To support these enterprise and business line objectives, the Trust Division will maintain an appropriate and comprehensive compliance and risk monitoring process.

First Line

SAMPLE PROCEDURE

Procedure: Risk Assessment

Risk Categories and component Risk Issues are assessed considering factors including but not limited to:

- Risk Control Self Assessments and other business unit self-assessments
- Complaints
- Loss History
- New products/services, emerging trends, laws, regulations, and regulatory guidance

Risk Categories and Risk Items will be risk-rated based on:

- Likelihood
- Severity
- Experience

First Line

SAMPLE COMPLAINT FORM

Client Name: _____ Account #:____ Account Type:_____

Nature of complaint issue (Investment, Product, Service, Administration, Privacy, Other):_____

Explain nature of concern:_____
Has the concern been resolved and how:_____

Is this indicative of a broader issue that could involve multiple clients that should be addressed globally?_____

Signatures: Account Officer_____ Management_____

First Line

SAMPLE LOSS FORM

Event:_____ Event Date:_____

Client Name:_____ Account #:_____

Account Type:_____ Business Unit:_____

Dollar Amount:_____ Recovery Amount, if any:_____

Event Description:_____

Root Cause/Thematic Issue*:_____

Impact:_____

Resolution:_____

Action Plan:_____

Risk Specialist:_____ Risk Manager:_____

Impact Analysis Participants:_____

*Basel II Op Risk Event Categories: Internal Fraud, External Fraud, Employment Practices and Workplace Safety, Clients/Products/Business Practice, Damage to Physical Assets, Business Disruption/Systems Failure, Execution/Delivery/Process Management

First Line

SAMPLE NEW ACTIVITIES REPORT*

New Activity:_____ Description_____

What is the rationale/demand for the product/activity?_____

Identify risks, concerns, and necessary controls associated with the activity:_____

Are the associated risks within the bank's strategic plan, risk profile, and risk appetite?_____

Are there unique/new laws or regulations to be considered? If so, identify/describe:_____

Will additional/new expertise be needed to manage the new activity?_____

Identify operational infrastructure, controls, and technology required for implementation:_____

Will Third Party service providers be needed and will due diligence be conducted?_____

Attach a business plan including:

Expected costs:_____

Sales revenue targets:_____

Performance or risk metrics:_____

Exit Strategy if metrics not met:_____

Management/Committee Approval_____ Date_____

* Standards from OCC Comptroller's Handbook, Corporate and Risk Governance July 2019

First Line

ANNUAL INVENTORY AND ASSESSMENT OF RISKS

Management and Business Line Stakeholders should:

- Review inventory of existing risks
- Identify any new or additional risks based on history (foregoing reports)
- Assign Inherent Risk rating based on: likelihood, severity, and experience
- Review/ Validate/ Risk Rate controls in place to address each risk item. Consider: operational/systems controls, procedures, First Line testing
- Assign Residual Risk rating
- Develop plan to control for each risk item
- Reassess/mid-year review if a significant event occurs

First Line

SAMPLE RISK INVENTORY AND ASSESSMENT

Line of Business	Risk Item	Inherent Risk	Controls/ID Type	Residual Risk
	List/evaluate each (Examples below)	L-M-H or 1-2-3	Strong-Mod-Weak	L-M-H or 1-2-3
Investments	Failure to follow IPS	2 Moderate	2 Mod/ Self Test	2 Moderate
	…			
Administration	Distribution Errors	2 Moderate	1 Strong/Procedure	1 Low
	…			
Operations	System Interface	3 High	1 Strong/System	2 Moderate
	…			
Legal/Regulatory	Regulatory Reports	3 High	1Strong/OrgStructur	2 Moderate
	…			
Other (list/itemize)	…			

Risk Rating Metrics*:

1 Low Unlikely (=< 1 per year), low $ impact (<100K)

2 Moderate Somewhat likely (1-20 times), moderate $ impact ($100K - $1M)

3 High Highly likely (>20 times), high $ impact (>$1M)

* $ amounts and frequency tailored to your Enterprise Risk Tolerance. Those shown here are illustrative only, and do not represent suggested limits, specific risk items, controls, or ratings at any particular institution.

First Line

DEVELOP/MODIFY RCSA PLAN

- ID/Develop Controls for Each Risk Item
- Prioritize H-M-L Risks
- Controls: “Don’t Reinvent the Wheel.” Leverage/adapt current tools.
  - Systems Safeguards (Trust System)
  - Process/Organizational Controls (Dual Controls, Centralized Independent Functions for Account Opening, etc.)
  - Procedures (Safeguards built into processes)
  - Testing
    - Automated exception reports (Daily reports of OD’s, trade errors, etc.)
    - Semi-automated exception reports and reviews (Apparent inconsistent coding)
    - Manual testing (Schedule sample of accounts to review for Discretionary Distributions, Adherence to IPS, ERISA Prohibited Transactions, etc.)
- Validate all controls periodically on a risk prioritized basis
- Escalate findings on Quarterly or Monthly Dashboard, including Direction of Risk

First Line

SAMPLE CONTROL INVENTORY

Line of Business	Risk Item	Inherent Risk H-M-L	Describe Control/Oversight/ Monitoring/ Surveillance Process	Additional Self-Testing Needed Y/N
	Example 1	H	None	Y
	Example 2	H	Procedure	Y
	Example 3	M	Centralized Account Opening Unit- Dual Control	N
	Example 4	L	Automated Exception Reporting	N

First Line

SAMPLE SEMI-AUTOMATED EXCEPTION REPORT

APPARENT INCONSISTENT CODING

Run systems coding report including:

Investment Authority:_____

Trade Authority:_____

Account Capacity:_____

Account Type:_____

Approved Inconsistency:_____

Date Inconsistency Approved (coded on system):_____

First Line

SAMPLE CONTROL EXAM TEST SUMMARY

Business Unit Reviewed:_____ Overall Rating:_____

Exam Conducted by:_____ Date:_____

Description of Focus: include number of accounts, topics, and processes reviewed:_____

Existing Controls/Surveillance/Oversight Processes:_____

Describe Sample and Methodology:_____

Areas/Topics Rated:_____

Risk Category:(list each)_____ Observations:(for each)_____

_____ _____

LOB Response if Needs Improvement or Unsatisfactory:_____

First Line
SAMPLE RCSA RESULTS

Risk Item	Test Completed	Risk Items	Inherent Risk	Residual Risk	Test/Report
Trade Processing	Date	4	2-H, 0-M, 2-L	0-H, 0-M, 4-L	Trade Processing
Estate Admin	Date	5	0-H, 2-M, 3-L	0-H, 1-M, 4-L	Tax Reporting, Court Accountings
Investments	Date	7	3-H, 2-M, 2-L	1-H, 3-M, 3-L	Reg 9, IPS
ERISA Prohibited Transactions	Date	3	3-H, 0-M, 0-L	0-H, 2-M, 1-L	Admin Reviews
… list each item					

Risk Rating Metrics*:

1 Low- Unlikely (=< 1 per year), low $ impact (<100K)

2 Moderate- Somewhat likely (1-20 times/year), moderate $ impact ($100K-$1M)

3 High- Highly likely (>20 times/year), high $ impact (>$1M)

* Risk Metrics $ amounts and frequency tailored to your Enterprise Risk Tolerance. Those shown are illustrative only, and do not represent suggested limits, specific risk items, controls or ratings at any particular institution.

First Line
SAMPLE DASHBOARD

	Previous Period	This Period	Direction of Risk
KRI's Breached	2	1	
New Laws/Regs/Trends	1	2	
New Products/Markets	1	1	
Operational Losses	$	$	
Other Performance Events	#	#	
Outstanding Regulatory Exam Issues	#	#	
Outstanding Audit Issues	#	#	
Outstanding Compliance Issues	#	#	
Self-Tests Completed w NI or Unsatisfactory Rating	#	#	
Overall RCSA Rating	H-M-L	H-M-L	

OVERALL DIVISION RISK RATING: MODERATE **OVERALL DIRECTION OF RISK:** Stable

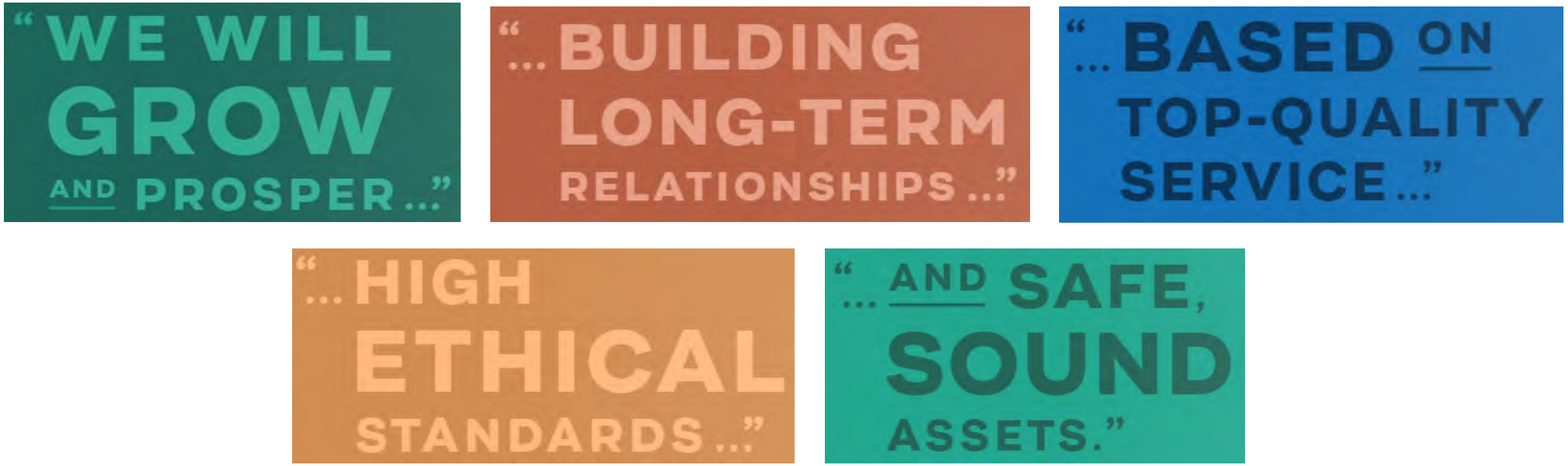
MAY 2, 2023 | FIRMA

Frost Bank

Second Line of Defense

The Frost Philosophy

…"because unless you back up your values with actions, they're just empty words."



INTEGRITY
CARING
EXCELLENCE

"We" refers to all employees engaging as a team.

"Our risk standards are high."

"We are prudent and proactive in managing operational, technology, credit and market risk."

FROST BANK

Enterprise Risk Management

Second Line of Defense

Three Lines of Defense

- 1st Line – **Line Management** – Provision of products and services to clients; manages risk through control ownership

- 2nd Line – **Risk Management** – Provides expertise, support, monitoring and challenge on risk-related matters

- 3rd Line – **Internal Audit** – Independent and objective assurance and advice on all matters related to the achievement of objectives

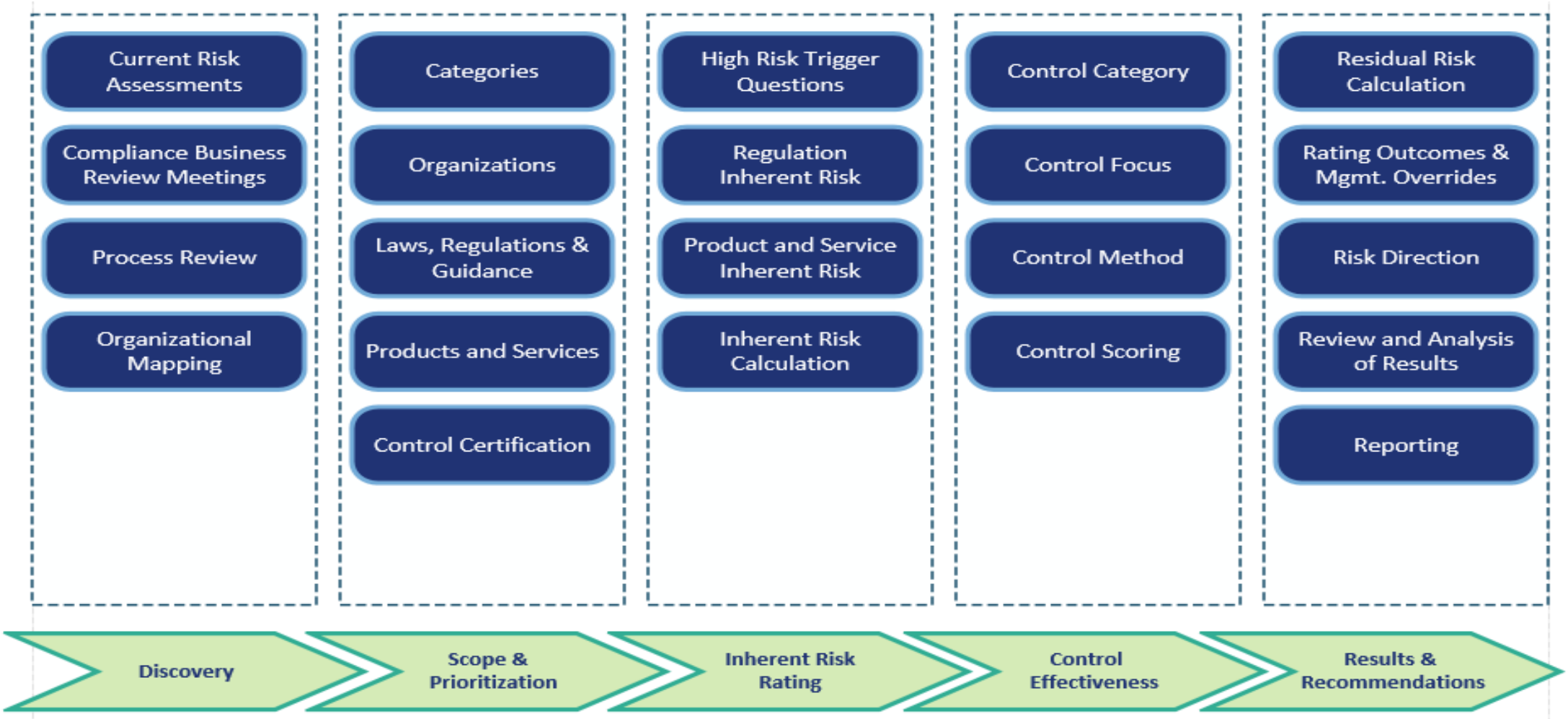
- SOURCE: Definitions taken from The IIA's Three Lines Model

New Organization

FROST BANK

Compliance Risk Assessment

Process Flow



Objectives

- Achieve an integrated and comprehensive understanding of how regulatory compliance requirements impact Frost, with a specific emphasis on the requirements of each section within regulations;
- Provide an effective and consistent process that evaluates and quantifies compliance risk across different processes, organizations, products, and services;
- Strengthen accountability and collaboration with the business lines and management; and
- Provide an effective way to plan and appropriately budget time and resources for monitoring and testing.

Scope – Annual Assessment

Fiduciary Compliance Regulatory Topic
FDIC Statement of Principles
FDIC Trust Examination Manual
Federal Reserve Handbook, Fiduciary Activities, Asset Management
Privacy of Consumer Financial Information
Protection of Vulnerable Adults from Financial Exploitation
Recordkeeping and confirmation of certain securities transactions effected by State member banks
Service Provider Guidance
Texas Estate Code
Texas Property Code State Laws on Trust and Fiduciary Activities
United States Code Title 26 – Internal Revenue Code
United States Code Title 29 Chapter 18
12 CFR 9.5 Policies and Procedures
12 CFR 9.8 Recordkeeping
26 CFR 1.6045A-1- Statement of information required in connection with transfers of securities

Inherent Risk Identification

Inherent risk considers the likelihood and impact of noncompliance with consumer laws and regulations prior to considering any mitigating effects of risk management processes (Source: Federal Reserve Board of Governors)

- Regulation Inherent Risk –
  - Impact – 5 questions
  - Likelihood – 4 questions
  - Respondent – Compliance
- Product/Service Inherent Risk
  - Impact – 6 questions
  - Likelihood – 9 questions
  - Respondent – Business
- Possible responses are assigned risk scores.
- “High Risk” questions are weighted heavier.

Control Effectiveness

Internal Control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.

Control effectiveness is the term used to describe how well a control is reducing or managing the risk it's meant to modify

- Control Focus
  - Preventive
  - Detective
- Control Method
  - Automated
  - Manual

Control Attribute Scores

Control Attribute Scores		Focus	
		Preventative	*Detective*
Method		1	5
Automated	1	1 - System Hard stop	3
Mostly Automated	2	1.5	3.5
Mostly Manual	3	2	4
Manual	5	3 – Procedures	5

Control Environment Score

Two Controls		Control 2 (method/focus)							
		Automated/ Preventative	Mostly Automated/ Preventative	Mostly Manual/ Preventative	Manual/ Preventative	Automated/ Detective	Mostly Automated/ Detective	Mostly Manual/ Detective	Manual/ Detective
Control 1 (method/focus)	Automated/ Preventative	1	1	1	1	1	1	2	2
	Mostly Automated/ Preventative	1	1	1	1	1	2	2	2
	Mostly Manual/ Preventative			2	2	2	3	3	3
	Manual/Preventative				2	3	3	3	3
	Automated/Detective				3	3	3	3	3
	Mostly Automated/ Detective						4	4	4
	Mostly Manual/ Detective							5	5
	Manual/ Detective								5

Residual Risk Score

5 point Scale	Control Environment Score	Residual Risk Reduction
1	Strong	2 levels
2	Satisfactory	1 level
3	Fair	1/2 level
4	Limited	0
5	Unestablished	0

*There's a floor value of 1, i.e. RR can't go below a 1.

Residual Risk Rating

Residual Risk Ratings	
Low	1-1.99999
Acceptable	2-2.499999
Moderate	2.5-3.99999
Elevated	4-4.49999
High	4.5-5.0

Monitoring and Testing

Residual Risk Rating	Testing Frequency
Low	Triennially (At least every 3 Years)
Acceptable	Biennially (At least every 2 Years)
Moderate	Annually
Elevated	Semi-Annually
High	Quarterly

Sampling Methodology

Control Method	Control Focus	Maturity of Control	Base Sample Size	Extended Sample Size
Manual	Detective	<12 Months	25 or 100% of Population	15
Manual	Detective	>12 Months	20 or 100% of Population	15
Manual	Preventative	<12 Months	25 or 100% of Population	15
Manual	Preventative	>12 Months	20 or 100% of Population	15
Mostly Manual	Detective	<12 Months	20 or 100% of Population	15
Mostly Manual	Detective	>12 Months	15 or 100% of Population	15
Mostly Manual	Preventative	<12 Months	20 or 100% of Population	15
Mostly Manual	Preventative	>12 Months	15 or 100% of Population	15
Mostly Automated	Detective	<12 Months	15 or 100% of Population	10
Mostly Automated	Detective	>12 Months	10 or 100% of Population	10
Mostly Automated	Preventative	<12 Months	15 or 100% of Population	10
Mostly Automated	Preventative	>12 Months	10 or 100% of Population	10
Automated	Detective	<12 Months	10 or 100% of Population	10
Automated	Detective	>12 Months	5 or 100% of Population	10
Automated	Preventative	<12 Months	10 or 100% of Population	10
Automated	Preventative	>12 Months	1 Test Case from each product and channel	5

Scope – Ongoing Assessment

The risk assessment is a tool to assist both Compliance and the lines of business in measuring and understanding compliance risk. Although a compliance risk assessment is performed annually, certain functional areas may require review on a more frequent basis, particularly if there is a significant legal or regulatory change that could potentially affect the organization such as:

- Emerging trends within the industry,
- Material changes in products or services;
- An upgrade, renewal, or implementation of internal software systems that materially affect the delivery of products and services; or
- Where monitoring or independent testing of business practices show material gaps or weaknesses.

Internal Audit

Third Line of Defense

Third Line
Internal Audit Risk Assessment

Audit Universe

Identify Auditable Entities (1st year development)

- Determine universe structure (process / business unit/strategic goals)

- Get inputs from key members of the management team and Risk Management to identify auditable entities

- Review financial results, business & process documentation, corporate strategic initiatives

- Audit Universe should be reviewed Annually (at least)

Risk Assessment

Conduct Risk Assessment

- Assess the audit universe against key elements (strategic, liquidity, compliance, operational risk, technology risk, etc.)

- Recommended alignment with enterprise risks

- Include both qualitative and quantitative data

- Assessment based on inherent and residual

Audit Plan

Develop Audit Plan

- Based on the risk of each entity, develop a 1-3 or 1-5 year audit plan

- Present assessment results to the Audit Committee for approval

- Reevaluate risk assessment as needed and update audit plan

Internal Audit Risk Assessment – Example

Audit Universe	(F1) Capital/Solvency/Business Risk	(F2) Credit Risk	(F3) Liquidity Risk	(F4) Market Risk	(F5) Model Risk	(NF1) Op Risk - Business Disruption and System Failure	(NF2) Op Risk - 3rd Party Dependency	(NF3) Op Risk - Facilities and Workplace Safety	(NF4) Op Risk - Customer Impact and Suitability	(NF6) Op Risk - External Fraud	(NF7) Reputation Risk	(NF8) Strategic Risk	(NF9) Legal Risk	Risk Score
ACH	2	2	1	0	0	3	2	1	3	3	2	1	2	57.46
ALLL	2	3	2	1	3	2	1	1	1	1	3	2	2	63.33
Appraisal	1	2	1	0	0	3	3	2	2	2	2	2	2	56.11
Automated Teller Machine (ATM)	0	0	0	0	0	1	1	1	2	1	1	0	1	30.1
Branch Program	3	1	0	0	1	3	3	3	3	3	3	3	2	61.51
BSA/AML and OFAC	3	0	0	0	3	3	1	1	2	2	3	2	3	65.33
BSA/AML and OFAC Risk Assessment	3	0	0	0	2	1	0	0	1	2	3	2	3	65.83
Business Continuity Management	2	0	2	0	0	3	1	3	3	2	3	1	2	69.17
Customer Care	2	0	0	0	0	3	2	1	3	2	3	1	1	63.33
Capital Planning and Stress Testing	3	2	2	2	3	2	1	1	1	1	2	2	1	58.97
Change Management	2	0	0	0	0	3	1	2	3	1	2	1	1	63.33
Commercial Banking and Services	2	1	1	1	0	3	1	1	3	2	3	1	2	62.08
Commercial Remote Deposit Capture	2	2	0	0	1	2	1	1	3	2	2	1	2	60.81
Compliance Function	3	0	0	0	2	3	0	1	2	2	3	3	3	72.74
Configuration and Asset Management	1	0	0	0	0	3	2	3	2	1	2	1	2	59.29
Corporate Services	2	0	0	0	0	3	1	3	2	3	3	1	1	69.67
Credit Review Function	2	3	1	1	1	1	2	1	1	2	2	2	2	54.52

How We Assess Risk

- Qualitative metrics to identify risk such as:
  - Impact on strategic goals of the bank
  - Experience and strength of management and personnel
  - Complexity of processes
  - Manual intervention vs. automated processes

- Quantitative metrics such as:
  - % of turnover and # of open positions
  - Portfolio growth
  - # of systems with high business continuity risk

Inherent Risk Assessment – Example

Risk Assessment should incorporate both qualitative and quantitative risk criteria. Listed below is an example of both quantitative and qualitative risk tied to a specific criteria assessment to determine the risk scoring.

Risk Assessment Area	Quantitative and Qualitative	Description	Risk Question	Risk Scoring	Criteria
Operational Risk - 3rd Party Dependency	Quantitative	Level at which process is dependent on external support (vendors, resources, systems) to be successfully completed.	To what extent is this process reliant on a 3rd party (outside the Bank)?	High	2 or more moderate risk or 1 high risk vendor(s) support a primary component in the process of control framework (excluding system/application vendors).
				Moderate	2 or more low risk or 1 moderate risk vendor(s) supports a primary component in the process of control framework (excluding system/application vendors).
				Low	1 low risk vendor supports a primary component in the process or control framework (excluding system application vendors)
Operational Risk - External Fraud	Qualitative	Level at which process uses, stores, and/or transmits sensitive and confidential data impacting the risk of external threats and attacks.	What is the level of the threat that an external party would be financially motivated to gain access or acquire data?	High	NPPI, financial or other confidential bank data is heavily processed and/or prevalent throughout the process/control framework
				Moderate	NPPI, financial or other confidential bank data is utilized but not material to the process/control framework
				Low	NPPI, financial or other confidential bank data is minimally processed and/or prevalent throughout the process/control framework

Internal Audit Plan – Example

20XX Bank Internal Audit Plan - 3 Year Assessment

Engagement Name	Audit Type	Last Audit	2022	2023	2024	Frequency	Budget	Risk Rating
CECL	Full Scope	2020	X	X	X	1	240	
Appraisal	Full Scope	2021	X		X	2	160	
Automated Teller Machine	Full Scope	2019	X			3	160	
Bank Operations and Services	Full Scope	2021		X		3	500	
Branch Program	Full Scope	2021	X		X	2	750	
BSA/AML and OFAC	Full Scope	2021	X	X	X	1	1000	
BSA/AML and OFAC Risk Assessment	Full Scope	2021	X	X	X	1	250	
Wealth Management	Full Scope	2021	X	X	X	1	400	
Business Continuity Management	Full Scope	2021	X	X	X	1	240	

Continuous Reassessment of Risk

- Periodic meetings with senior management
- Periodic meetings with regulators and new/changing regulatory guidance
- Changes
  - New or modified systems
  - Rapid growth of portfolio
  - New products of LOBs
- Unexpected events resulting in increased or decreasing risk
  - Deposit runoff – SVB
- Concerns identified through Continuous Monitoring or Breaches of Key Risk Indicators (KRIs) or Risk Indicators (RIs)
- Review of results from 1st and 2nd line testing teams
- Changes in risk rating may result in changes in frequency of audit; changes are communicated to the Audit Committee for approval

Risk-Based Rotational Scope – Engagement Level

Risk-Based Rotational Scope: In addition to a risk-based internal audit plan, a risk based rotational scope can also be applied at the engagement level. Internal auditors can more accurately tailor the audit approach to current risks of the organization. Most often, this is applied to audits that are on a 1-2 year audit cycle.

Key Considerations:

- Detail and assess each process and risk that could be audited within engagement. Inherent and residual may be assessed
- Document rationale when assessment is more qualitative
- Detail in the Audit Announcement Memo what is in and out of scope
- Share with the business to get their perspective on risk level

Audit Name: 20XX Wealth Management Engagement
Prepared by:
Reviewed by:

Risk Assessment								Scoping Assessment							
Audit Scope/Program	Business Process	Enterprise Key Risk (if applicable)	Risk Description	Likelihood	Impact	Inherent Risk Level	Inherent Risk Rationale	Tested by 1st/ 2nd Line Assurance Function	Last Audit Year	Prior Year Audit Rating	Rotation Schedule (1-3)	Included in 20XX Scope	Included in 20XX Scope	Included in 20XX Scope	Scope Rationale 2022

Risk-Based Rotational Scope – Rating

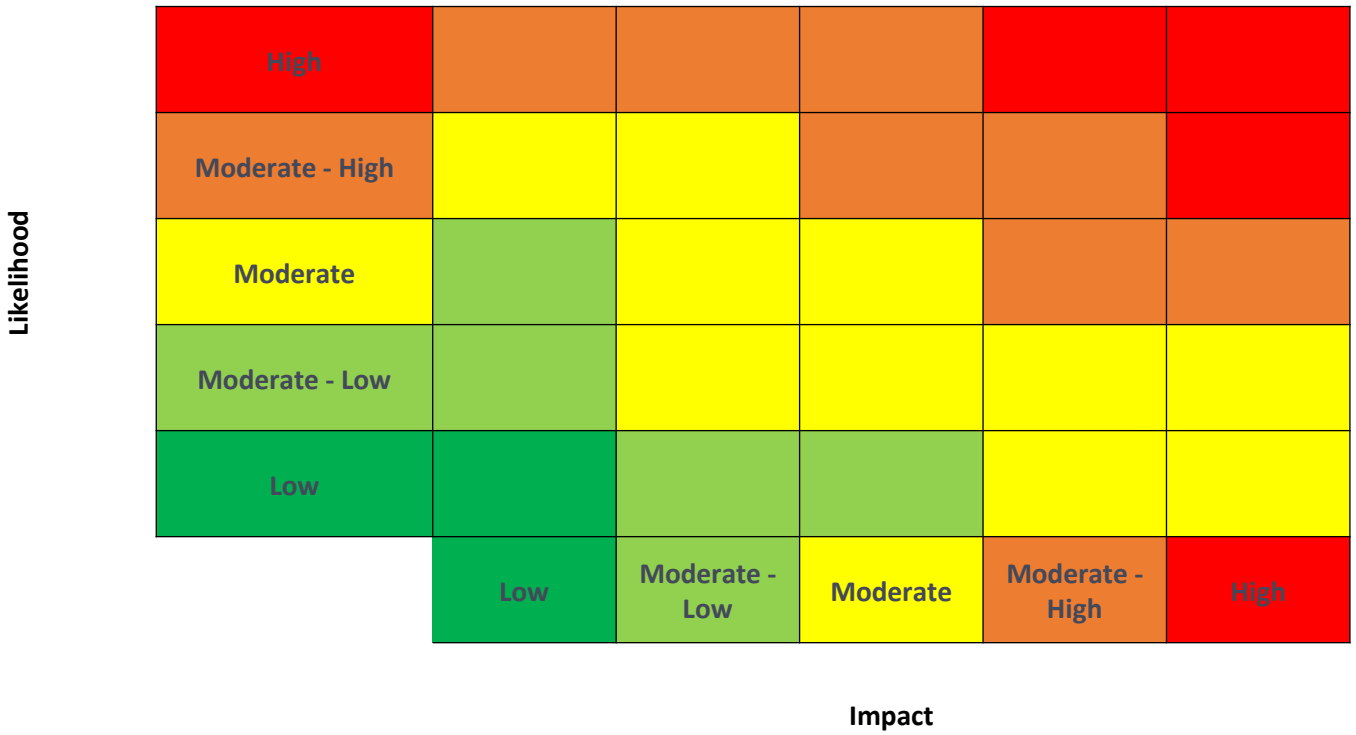
Level	Rating	Likelihood that Risk Will Occur
5	High	The risk is expected to significantly impact the bank in most circumstances
4	Moderate - High	The risk is likely to significantly impact the bank
3	Moderate	The risk is likely to have a more than a low but less than likely chance of being significant
2	Moderate - Low	The chance of the risk have a significant impact is slight
1	Low	The risk may occur and be significant only in rare circumstances

Level	Rating	Impact if Risk Occurs
5	High	Severe financial, reputational or other loss that ultimately could jeopardize the ability of the bank to continue without major changes. May require customer and regulatory communication.
4	Moderate - High	High financial, reputational or other loss and scrutiny by board. May require additional resources, immediate attention of senior management and/or a project plan.
3	Moderate	Requires management attention and could be a factor in not meeting budget expectations or strategic goals.
2	Moderate - Low	Minor impact that can be remediated without additional resources and does not impact strategic goals of the business.
1	Low	Business impact easily mitigated

Risk-Based Rotational Scope – Rating

Key Considerations:

- Likelihood and Impact should drive an overall inherent score to determine the rotational frequency.
- Areas rated high risk should always be included in scope
- Risks rated low inherently should be evaluated to determine the necessity of their inclusion
- All rationale should be documented and retained



Inherent Risk Rating	Rotation Cycle
High	1 Year
Moderate - High	1-2 Year
Moderate	2 Year
Moderate - Low	3 Year
Low	Why Testing?

Risk-Based Rotational Scope – Example

Audit Name: 20XX Wealth Management Engagement

Prepared by:

Reviewed by:

Risk Assessment								Scoping Assessment							
Audit Scope/Program	Business Process	Enterprise Key Risk (if applicable)	Risk Description	Likelihood	Impact	Inherent Risk Level	Inherent Risk Rationale	Tested by 1st/ 2nd Line Assurance Function	Prior Audit Year	Prior Year Audit Rating	Rotation Schedule (1-3)	Included in 20XX Scope	Included in 20XX Scope	Included in 20XX Scope	Scope Rationale 20XX
Trust Operations	Sales Incentive		Referral payouts are not in accordance with policy or referrals are not properly calculated or paid.	Medium	Medium	Medium	Based on XXX…	Yes	20XX	Satisfactory	2	N	Y	N	Based on XXX… we determined the item will be on a two year rotational scope.
Trust Operations	Regulatory Compliance		Non-compliance with Regulation R The Division does not conduct an annual analysis as of December 31st or does not accurately calculate the chiefly compensated test, and submit to Compliance within 60 days after the end of the prior calendar year to represent the Division's total compensation for Reg R analysis. The Bank does not consider all activities in its assessment of its applicability to Regulation R exceptions.												
Trust Administration	Daily Administration		The Bank does not administer the trust according to the terms in the trust document or in the best interest of the beneficiaries.												
Trust Administration	Assest Management		Assets within the estate are lost, stolen or fall into disrepair.												
Trust Administration	Dormant Accounts		The division does not monitor dormant accounts, make reasonable attempts to contact account owner(s)												
Investment Management	Investments Management		Trust investments are transacted that are not in accordance with documented trust authorities or in accordance with approved investment goals/guidelines of the respective trust account.												
Trust Open and Closed Accounts	Closed Accounts		Trust assets are not transferred to the trustor/grantor/beneficiary properly or on a timely basis. Trust accounts are not properly closed in accordance with trust policies and procedures and governing instruments												

Audit Scope Risk Assessment – Example

Audit Name: 20XX Wealth Management Engagement

Prepared by:

Reviewed by:

Risk Assessment								Scoping Assessment							
Audit Scope/Program	Business Process	Enterprise Key Risk (if applicable)	Risk Description	Likelihood	Impact	Inherent Risk Level	Inherent Risk Rationale	Tested by 1st/ 2nd Line Assurance Function	Last Audit Year	Prior Year Audit Rating	Rotation Schedule (1-3)	Included in 20XX Scope	Included in 20XX Scope	Included in 20XX Scope	Scope Rationale 2022

Questions