2022 FIRMA National Risk Management Training Conference

May 3, 2022

Nashville, Tennessee

Risk Assessment and the Three Lines of Defense

Joan Dindoffer
Carol Severyn
Natalie McCabe

Three Lines of Defense

WHO is responsible for risk management?

- First Line: Front Line Units / Business Units
  - Unit generates revenue or provides operational support or IT to revenue generating unit
- Second Line: Independent Risk Management (IRM)
- Third Line: Audit

EACH HAS A DISTINCT BUT COMPLEMENTARY ROLE

Proviso

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
- No "one size fits all"
- Purpose- to identify, assess, control, measure, monitor, & report risks

Front Line Units

First Line of Defense

First Line

WHAT are the responsibilities of the First Line?

- Assess, on an ongoing basis, material risks of the business through Risk Self Assessments
- Policies- Establish policies so that front line risk is:
    - Identified
    - Measured
    - Monitored
    - Controlled
    - Consistent with Bank's Risk Appetite Statement and within Risk Governance Framework

First Line

First Line Responsibilities (cont.)

- Procedures and processes to comply with policies
- Adhere to all applicable policies, procedures, and processes established by the Second Line
- Develop, attract, and retain talent

FIRST LINE OWNS RISK!

First Line

WHY the First Line has key responsibility for risk:

- Business units best understand the guidelines under which they operate and have accountability for all risk-taking and risk management activities that impact P&L and balance sheet
- Subject matter experts (SMEs) are familiar with fiduciary duties, laws, and regulations and understand new and existing risks within the industry and bank strategic initiatives

First Line

HOW does the First Line accomplish this?

Risk Control Self-Assessments (RCSAs), initially:

- Considerations in developing RCSAs, KRIs, Policies, and Assessments
    - Loss History
    - Complaints
    - New Laws
    - Emerging Trends
    - New Products/Services
    - Audit & Exam Issues
    - Media Reports & Reported Cases

First Line

RCSAs (cont.)

- Estimate
  - Likelihood
  - Frequency
  - Experience: Audit/exam findings, losses, regulatory change
- Metrics
  - High-Medium-Low, 1-5, or Red-Yellow-Green
  - $ amount and frequency within risk tolerance & limits established/reviewed by Second Line

To determine INHERENT RISK

First Line

RCSAs (cont.)

- Identify Inherent Risks- Product of consequence X likelihood
- Identify Controls for each
  - Policies & Procedures
  - System & Process Controls
  - Training
  - LOB Monitoring, Reporting, & Escalation
  - Testing/Self-Assessments
  - Rate Controls: Strong, Moderate, Weak
- Determine Residual Risk
  - Multiply/Overlay Inherent Risk by Controls
  - Product of Inherent Risk X Control Risk

INHERENT RISK minus CONTROLS = RESIDUAL RISK

First Line

Ongoing RCSA Process:

- Annually (or when a significant event occurs) reassess:
  - Identified Risks
  - Level of Risk
  - Controls in place & effectiveness
  - Direction of risk for each item & in the aggregate for the LOB
  - Action plan required
    - High – Immediate
    - Moderate – Monitored as part of risk program, but generally annually
    - Low – watched/monitored in some manner annually, but not necessarily annual testing

First Line

Management responsible for promptly:

- Correcting deficiencies found by Second Line, Audit, & regulators
- Escalating material issues
- Determining appropriate risk strategies & controls

First Line

Responsibilities

- Key Risk Indicators (KRIs) – Identify with metrics, limits, and direction
- Develop/strengthen policies & procedures to address all material/key risks with metrics consistent with risk limits contained in Bank's Risk Appetite Statement & Risk Governance Framework (or limits reviewed/challenged by Second Line) & review key policies annually
- Assessment – Test & Monitor
- Report KRI status & breaches & assessment results
- Train on key risks – talent development

First Line

Assessments

- Don’t reinvent the wheel. Leverage existing tools & practices
- Automated testing utilizing systems. Run exception reports, i.e.
    - Overdrafts
    - Trade Errors
    - Incompatible Investment Authority & Account Type Coding
- Account reviews (admin & Reg 9) may be leveraged to review for issues depending on independence of reviewer, or selective sample testing of reviews
- Design assessments to sample test other items not covered above, i.e.
    - Discretionary Distributions
    - Adherence to IPS
    - Co-trustee approvals
- Risk rate urgency of testing; highs at least annually
- Monitor for breaches & trending

First Line

WHERE & WHEN to Report

OCC requires reporting risks to all relevant parties at a frequency that meets their needs for decision making purposes

- To LOB Senior Management, at least Quarterly
  - Breaches of Risk Limits
  - Categorized by severity & impact to bank
  - Exception reporting & exception approval, to department/management committee
  - Status of resolution of identified issues
  - Trending of risks
- To Second Line
  - Ongoing meetings to determine corrective action status
  - Quarterly summary report/dashboard for further transmission to Board risk committee
- To Board
  - First Line should report material risks & events to Board fiduciary committee through management committees as they occur
  - Second Line should pass through/escalate Risk Dashboard/Summary Report of First Line to Board risk committee through Second Line committee structure Quarterly or Semi-Annually

First Line

Dashboard

A quarterly dashboard may be the best way to incorporate all required information, including:

- KRIs & status
- Self-Assessment test results
- Status/resolution of Compliance, Audit, & Regulatory Exam Issues
- RCSA & Risk Assessment Plan
- Trending & Overall Risk Evaluation/Score

First Line: It All Comes Full Circle

Frost Bank

Second Line of Defense

The Frost Philosophy

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

"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."

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

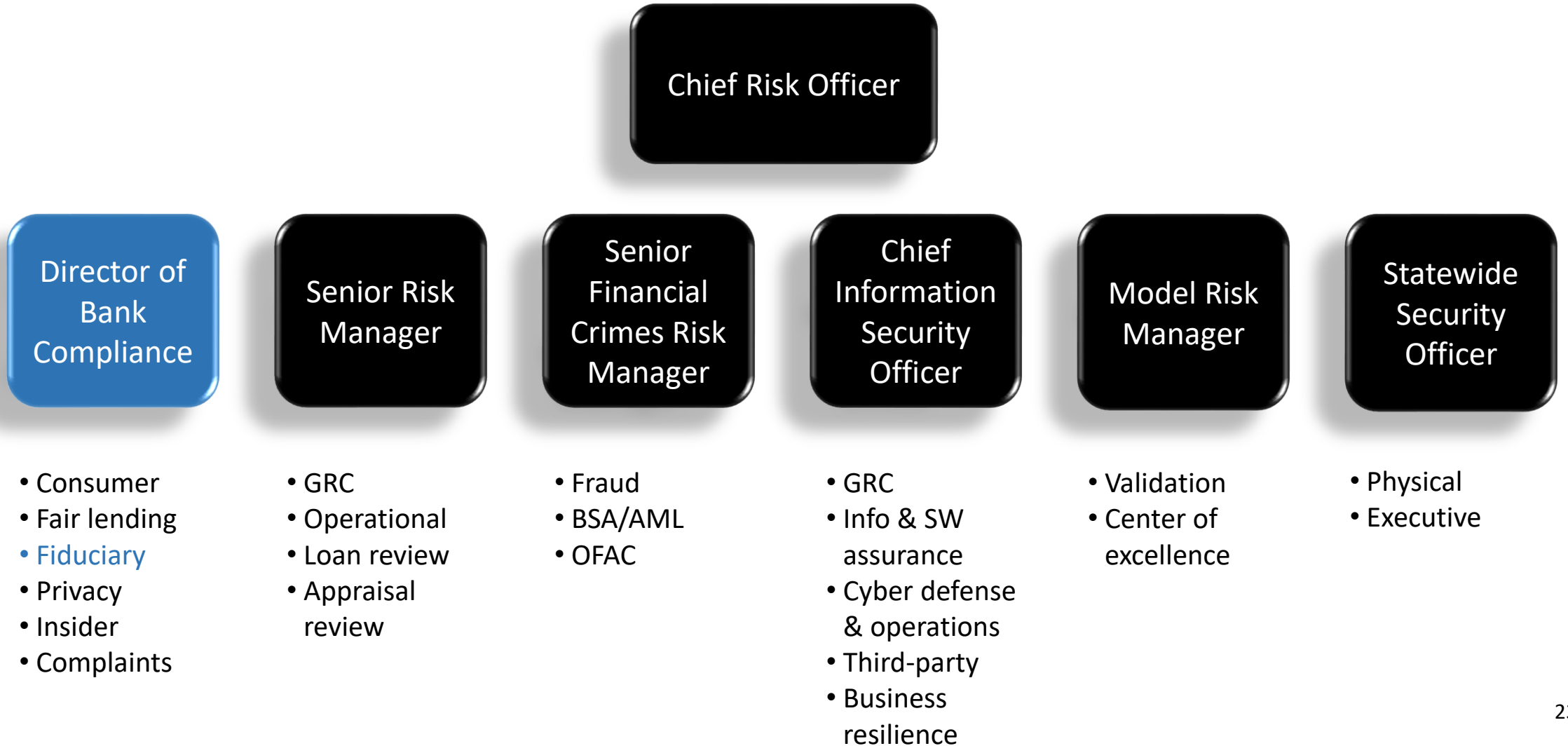
- 3rd Line – **Internal Audit** – Independent and objective assurance and advice on all matters related to the achievement of objectives

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

Risk Management

- Reorganization February 2019
- Bifurcated from credit risk
- New Chief Risk Officer
- Consolidated risk functions from all LODs
- New Priorities
  - Coverage
  - Consistency
  - Reporting
  - Maturity

New Organization

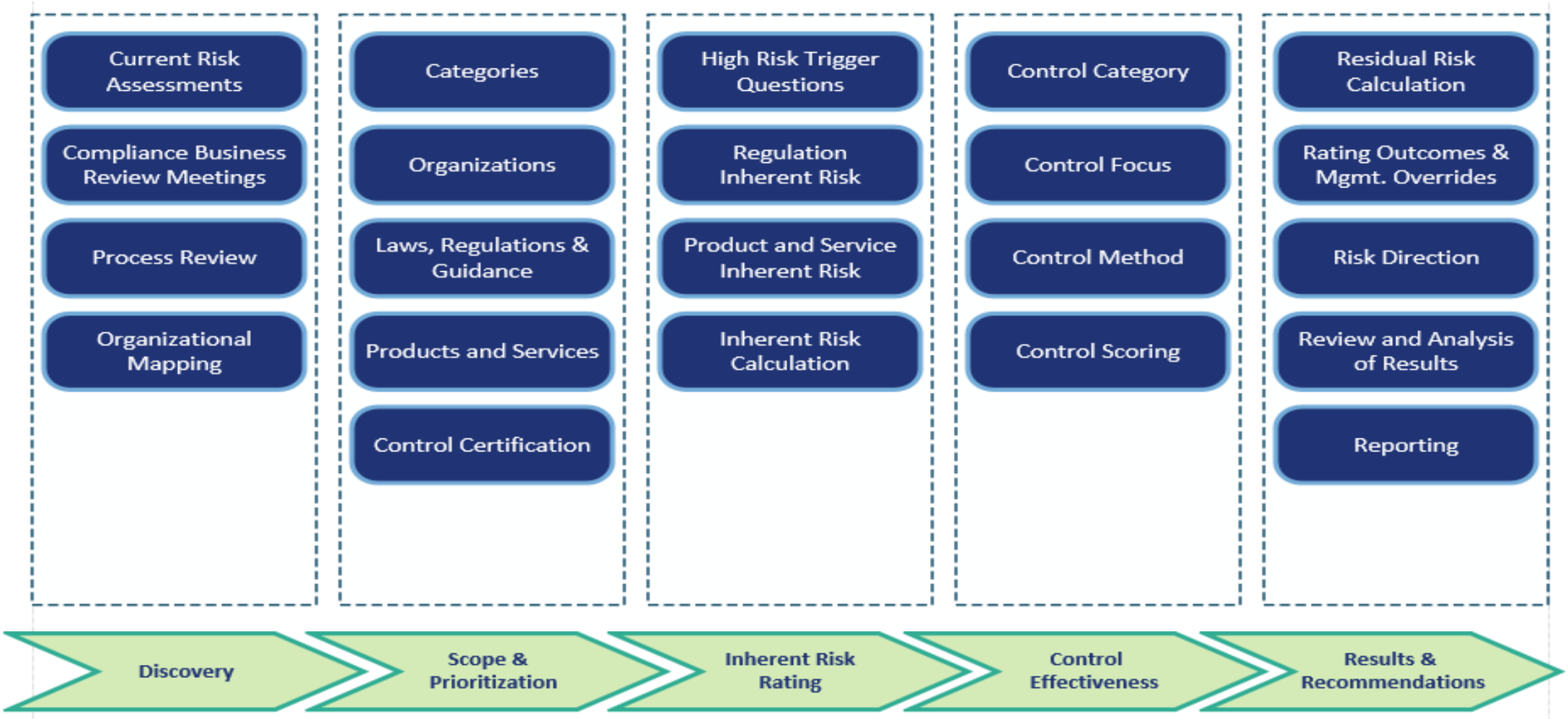


Compliance Risk Assessment

Methodology

- The risk assessment is a tool to assist both Compliance and the lines of business in measuring and understanding compliance risk.
- Frequency
  - Emerging trends
  - Material changes in products or services
  - Software changes
  - Gaps or weaknesses identified
  - Annual refresh
- Disciplined approach

Process Flow



Examples

Category	Product/ Service Name
Bank Compliance	Commercial CD Account
	Commercial Checking Account
	Commercial Credit Card
	Commercial Loans
	Commercial Money Market Account/ Savings Account
	Commercial OD Services
	Consumer CD Account/ IRA Ac
	Consumer Checking
	Consumer Debit Card

SAMPLES

Regulation Theme	Regulatory
Accuracy of Consumer Loan Applications	Reg B- Collection of GMI
	Reg B- General Rules
	Reg B- Joint Intent
	Reg B- Record Retention
Adverse Action Notices	Reg B- Requests for Information
	Reg B- Adverse Actions and Withd
	FCRA- Requirements on users of cc

Product Inherent Risk Questions and Responses				
#	Category	Question	Responses	High Risk Trigger
14	Impact	**Legal Activity - Industry / Bank:** Describe the nature of legal activity (e.g., settlements, litigation, and class action) in association with the product or service in the last 12 months.	No legal activity in the industry or at the institution	Yes
			Industry has moderate legal activity	
			Significant legal activity within the industry	
			The product is involved with recent or current legal issues at the institution*	
15	Likelihood	**Profitability and Benefits - Bank:** Describe the value of this product/ service in relation to the cost. Consider the frequency to which the consumers avail themselves of the benefits.	Low cost and high value	No
			Moderate cost and moderate value.	
			High cost and low value	

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

Results

- Drives monitoring and testing
- Frequency
  - Annual requirements
  - Automated versus manual controls
  - Material changes in products or services
  - Software changes
  - Gaps or weaknesses identified
- Disciplined approach
  - Test procedures
  - Root cause analysis
  - Issue tracking

Management Reporting

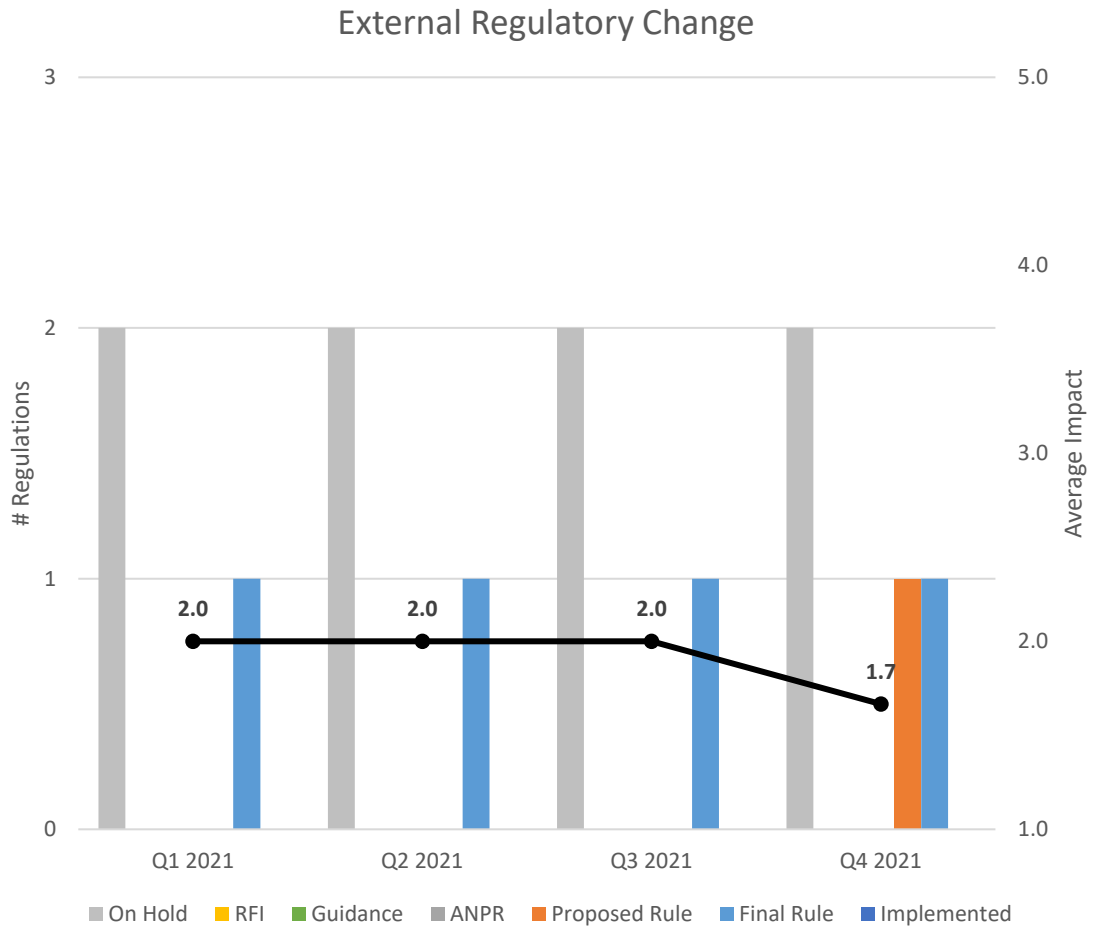
Emerging Risks

- Examination status and results
- Significant audit findings
- Emerging risks

External Regulatory Change

<TITLE>

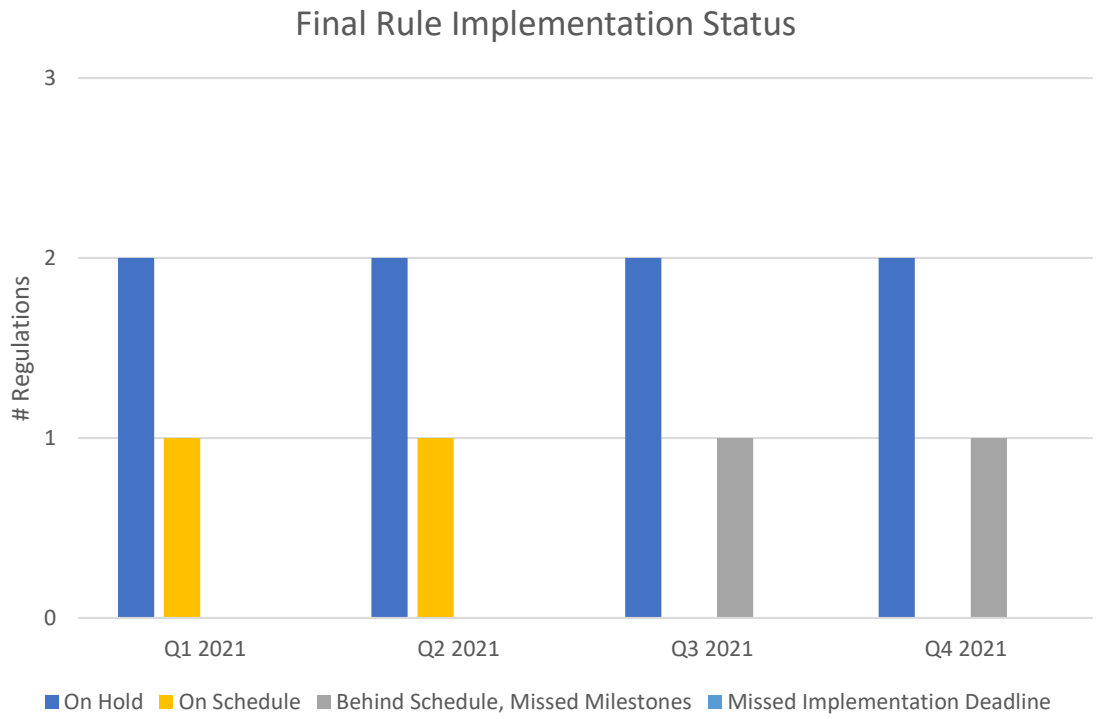
- Description and key requirements
- Estimated impact
- Mandatory compliance date
- Project description and timeline



External Regulatory Change

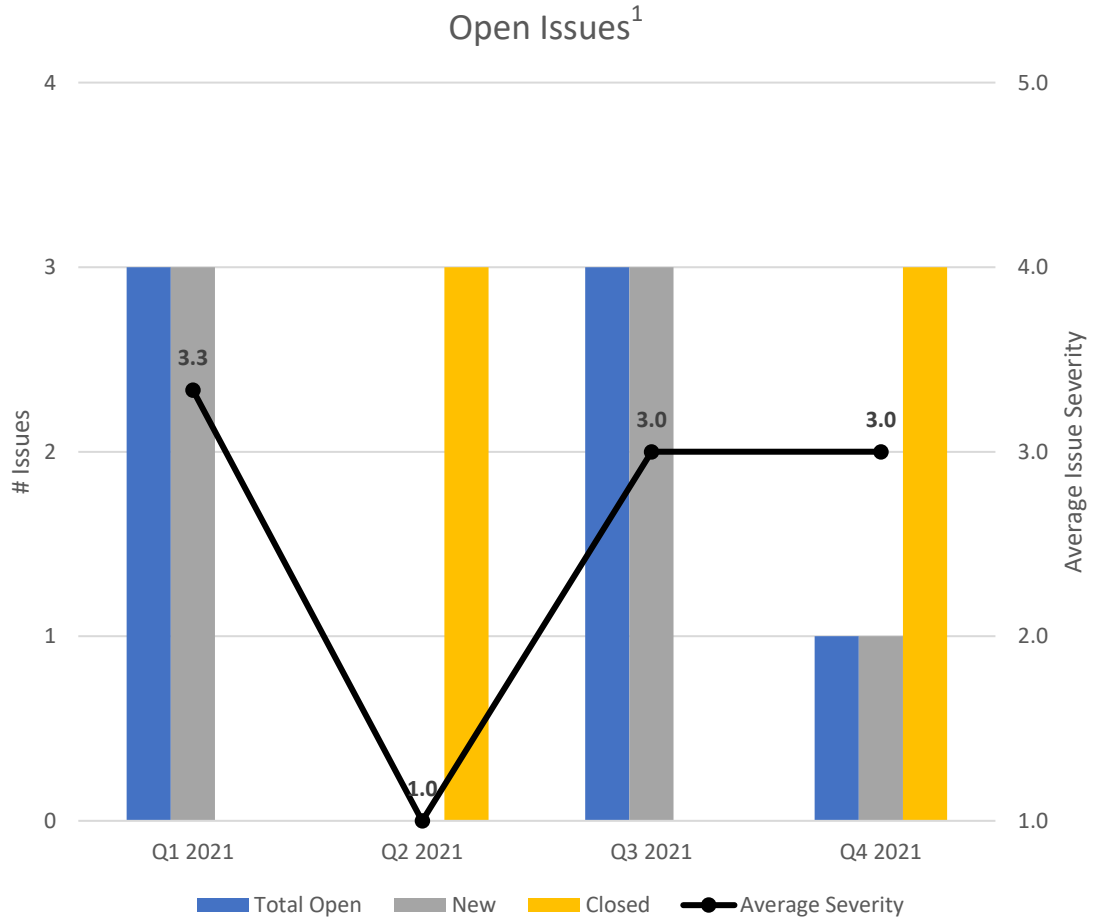
Final Rule Implementation Status

- Details #1
- Details #2
- Details #3



Issues Management

- <XX> issues were closed on schedule during the quarter.
- <XX> issues with extended remediation plans.
- <XX> new issues with a <LEVEL> rating were identified:
  - Issue #1
  - Issue #2
  - Issue #3

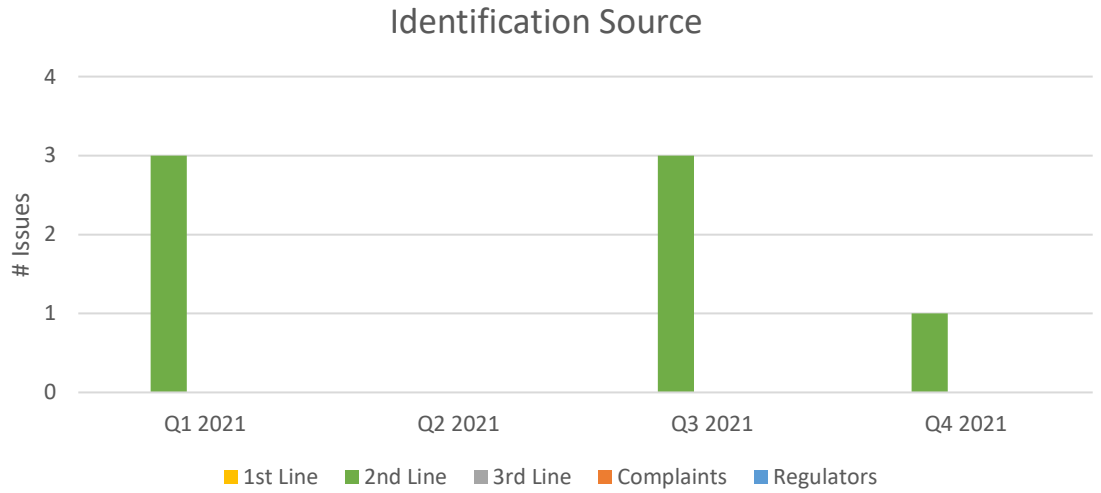


[1] Includes Issues with a severity of Moderate, Elevated or High

Issues Management

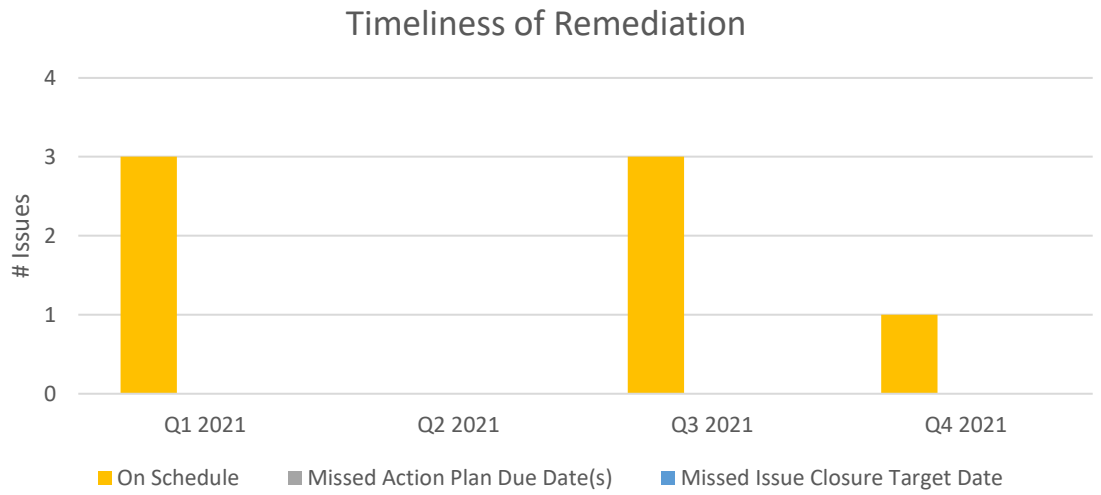
Identification Source

- Issues are identified by the line of business (1st line), through compliance monitoring and testing (2nd line), by internal audit (3rd line), through customer complaints, and regulatory examinations. Risk increases the further the identification of the issue is from the 1st line.
- Details #1
- Details #2
- Details #3



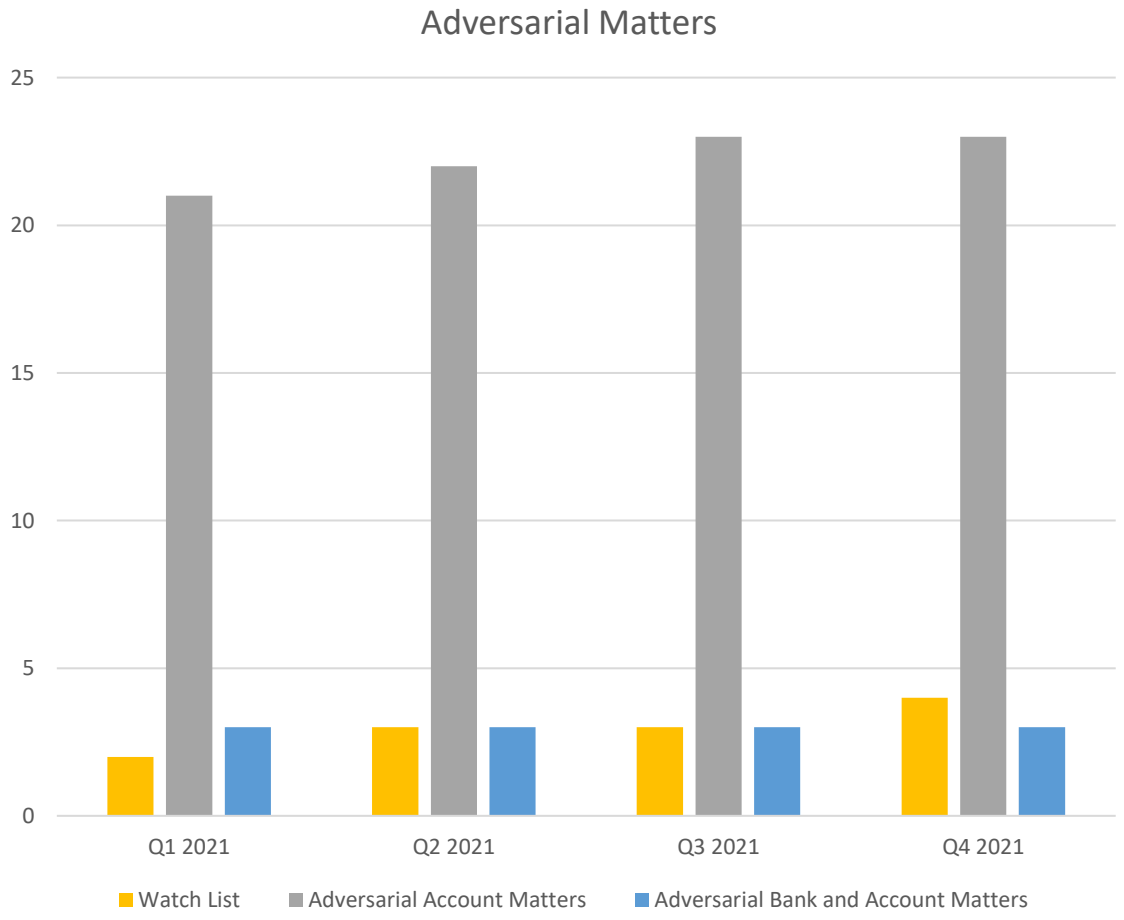
Timeliness of Remediation

- <XX> previous issues were remediated and closed out.
- <DESC> issue will not be remediated by the target date due to <DETAILS>.
- Remaining issue has a target date of closure <DATE> and is on schedule.



Adversarial Matters

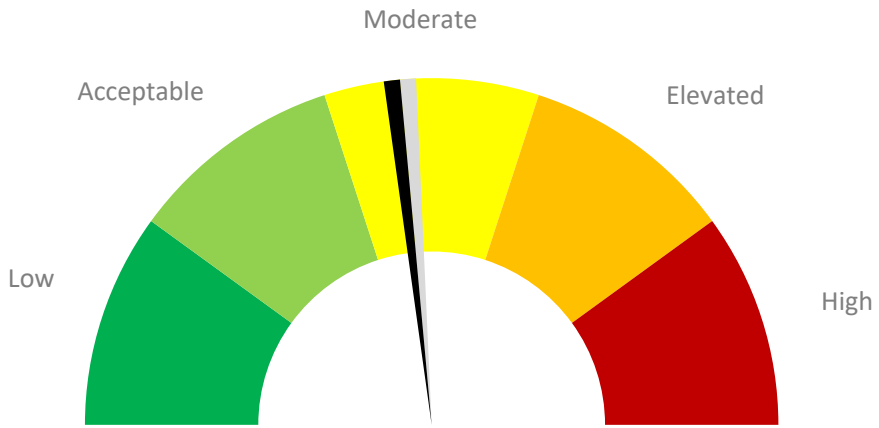
- Adversarial Matters remain relatively flat. One new Watch List item is being monitored.
- The Adversarial Matter against the Bank and Account concerning breach of fiduciary duties is in active remediation. Arbitrators were selected and the Plaintiff then filed an objection to the Arbitrators selected.



NOTE: Adversarial Matters against the Bank and Account are tracked by our internal Legal team.

Risk Committee Reporting

Compliance Risk



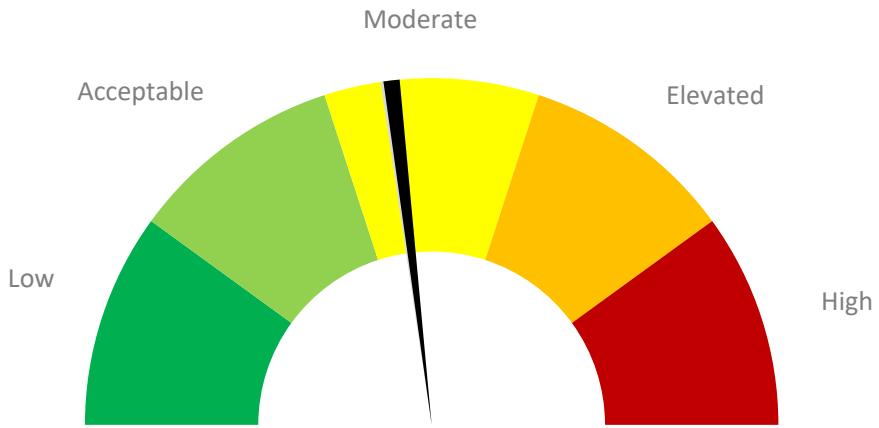
Stable

Overall Risk Summary

- Aggregate compliance risk remains <LEVEL> and <DIRECTION>
- Results of key risk indicators included in determination of aggregate compliance risk
- Including specific drivers from each subcategory

Rolling 4 Quarters
Current Period

Fiduciary Compliance



Emerging Risk
- Brief description

Issue Management – <LEVEL>, <DIRECTION>
- Key point #1
- Key point #2
- Key point #3

Regulatory Change – <LEVEL>, <DIRECTION>
- Key point #1
- Key point #2
- Key point #3

Adversarial Matters – <LEVEL>, <DIRECTION>
- Key point #1
- Key point #2
- Key point #3

Rolling 4 Quarters
Current Period

Internal Audit

Third Line of Defense

What is Internal Audit?

- Internal Audit is an independent, objective assurance & consulting activity, designed to add value & improve an organization's operations.

- Internal Audit reports directly to the Audit Committee instead of Bank management to promote transparency and avoid conflicts of interest. By remaining independent and objective, Internal Audit can provide an unbiased assessment of the overall health of the Bank.

- Internal Audit helps an organization in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate & improve the effectiveness of risk management, control & governance process.

- Internal Audit provides reasonable assurance to the Board of Directors and Senior Management that processes are working as they should be and risks are identified, monitored and managed.

What does Internal Audit Do?

Internal Audit performs the following activities:

- Audits of key functions/processes
- Continuous monitoring of key functions/processes/metrics
- On-going risk assessment
- Committee Involvement
- Account Management
- Quarterly reporting to the Audit Committee
- Consulting and Advisory

What is a Risk-based Approach?

Because there are so many functions and processes at the Bank and a limited number of resources and time, Internal Audit's goal is to focus on the areas of highest risk on an annual basis, while covering all processes over a prescribed period of time based on risk to the Bank.

Why is an Effective Risk Assessment Important for the Internal Audit function?

Internal Audit is governed by the mandatory elements of The Institute of Internal Auditor's (IIA's) International Professional Practices Framework (IPPF):

- IIA Standard 2010: requires "The chief audit executive must establish risk-based plans to determine the priorities of the internal audit."
- IIA Standard 2010.A1/A2: requires that "The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process"
- IIA Standard 2020, "The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations."
    - Interim changes to IA plan can be driven by changes to the risk assessment

Three Lines of Defense

External Audit

Internal Audit

3rd Line of Defense
Independent challenge to the levels of assurance provided by Business Units, Risk Management and oversight functions

Risk Management

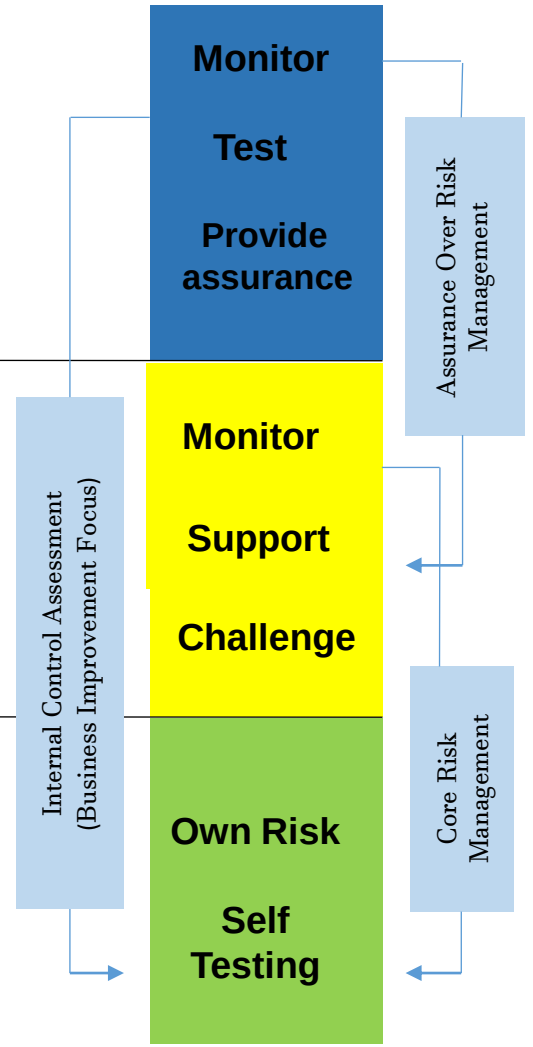
Oversight Functions

2nd Line of Defense
Provides expertise, support, monitoring and challenge. Oversight functions may also set directions, define policy and procedures, and have functional oversight

Line Management

Business Units

1st Line of Defense
Business operations which perform day to day risk management activity; manages risk through control ownership




Financial
Concentration
Model
Risks
Credit
Market
Transaction
Reputational
Interest Rate
Operational
Conduct
Compliance

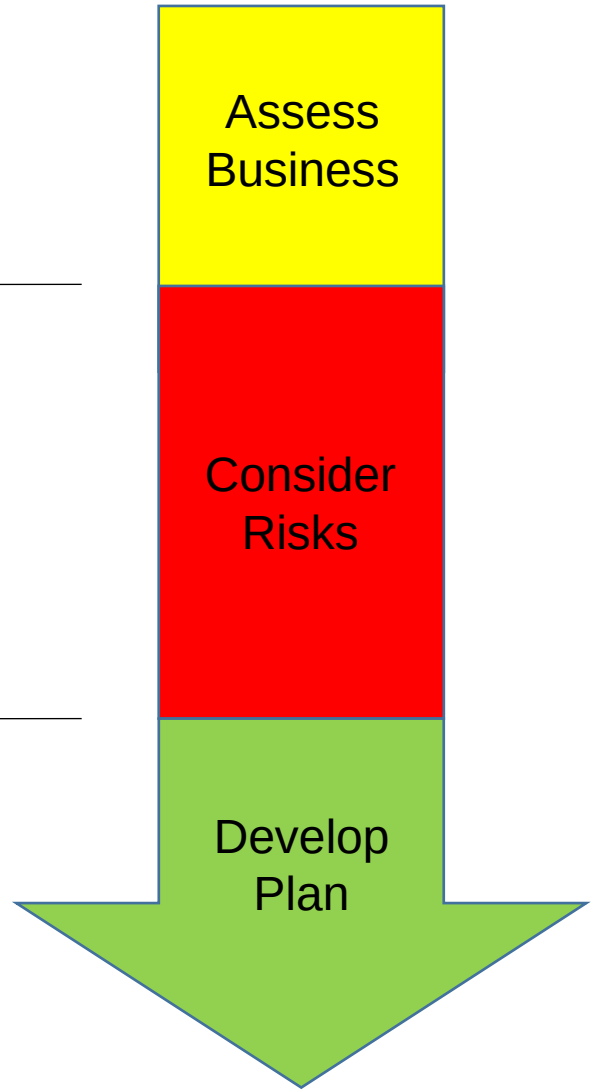
Internal Audit Risk Assessment

- Get inputs from key members of the management team and Risk Management
- Review financial results, business & process documentation, corporate strategic initiatives during current & prior years
- Review self-assessments performed by the business units and risk reporting from Risk Management and other oversight functions

---

- Inherent risk of business activity
- Current & anticipated business changes
- Financial/transaction significance & trends
- Current control environment: staffing, policies, culture, changes
- Degree of legal/regulatory compliance requirements

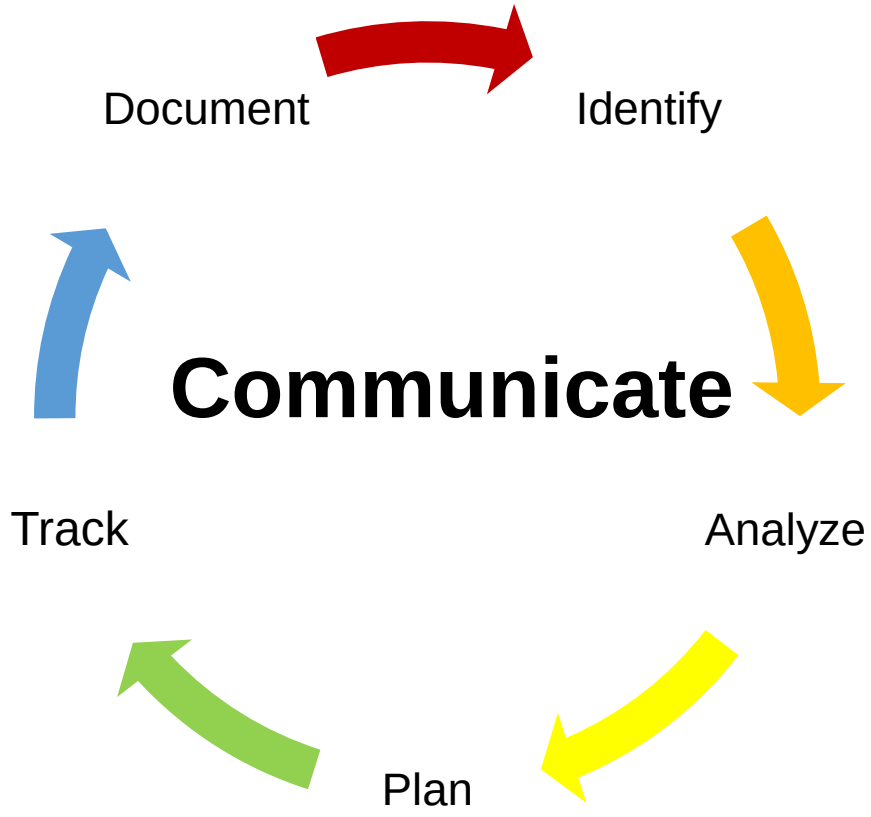
- Summarize results of risk assessments based on *Significance & Likelihood*
- Present assessment results to the Audit Committee for approval
- Finalize internal audit plan for the year
- Reevaluate risk assessment as needed and update audit plan



Risk Assessment

Internal Audit initiates the risk assessment through a combination of:

- Conducting interviews with business leaders to understand key strategic business objectives & each leader's view on organizational risks
- Understanding key points & risk considerations from an Enterprise Risk Management perspective
- Utilizing results from prior year audits, regulatory exams & other testing assurance function reviews



Inherent Risk Rating
(Risk without Mitigation/Controls)

Impact			
Rating	**Financial**	**Reputational**	**Regulatory**
5	X > $1B	Long-term impact to Bank	Regulatory shutdown
4	$1B > X > $100M	Significant impact to Bank	Regulatory probation/ongoing scrutiny
3	$100M > X > $10M	Manageable Negative publicity	Regulatory warning letter or equivalent
2	$10M > X > $500K	Publicity, no action necessary	Advisory letter
1	$500K > X	No publicity	No regulatory enforcement interest

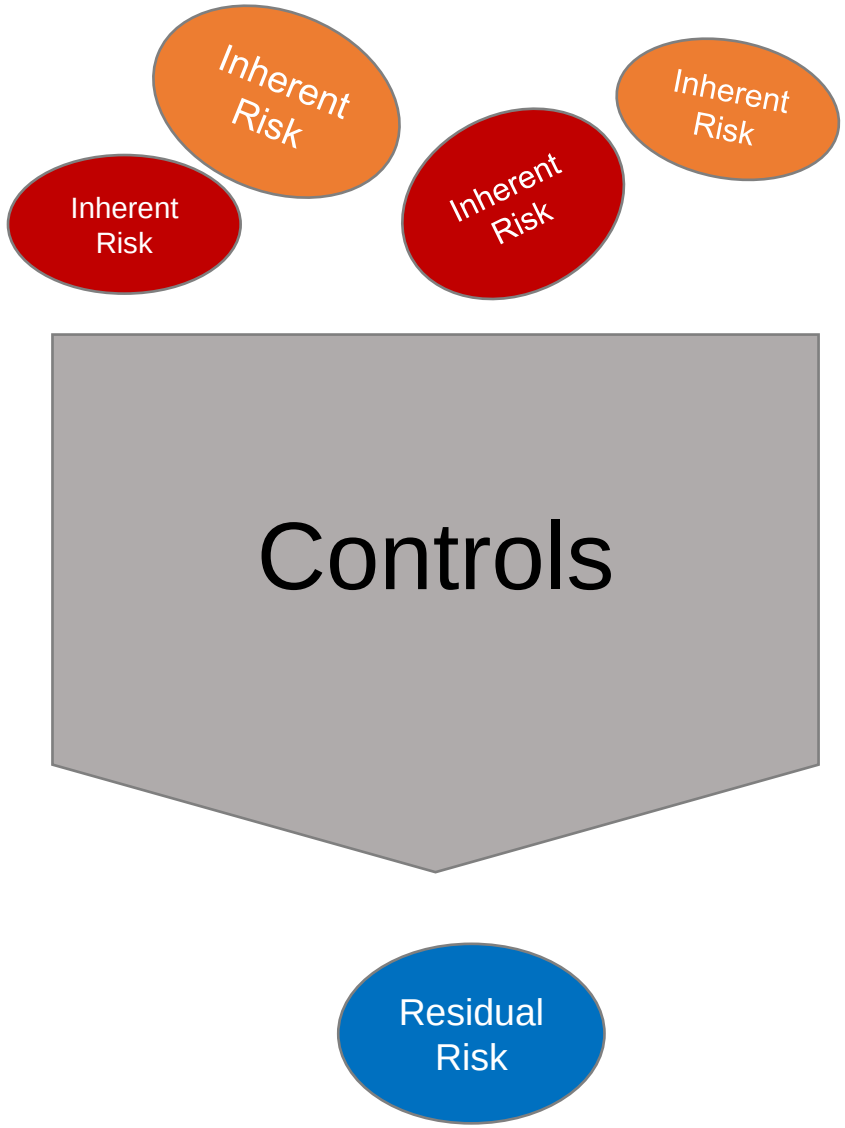
Rating	**Likelihood**
5	Frequent/routine occurrence
4	Likely
3	Occasional or possible
2	Unlikely - Seldom but not rare”
1	Rare

Key Points:

- Assess impact based on highest risk category
- Assess likelihood without existing controls or plan
- Inherent risk score = impact X likelihood

Determining Residual Risk

Residual Risk is the risk remaining after the controls are considered.

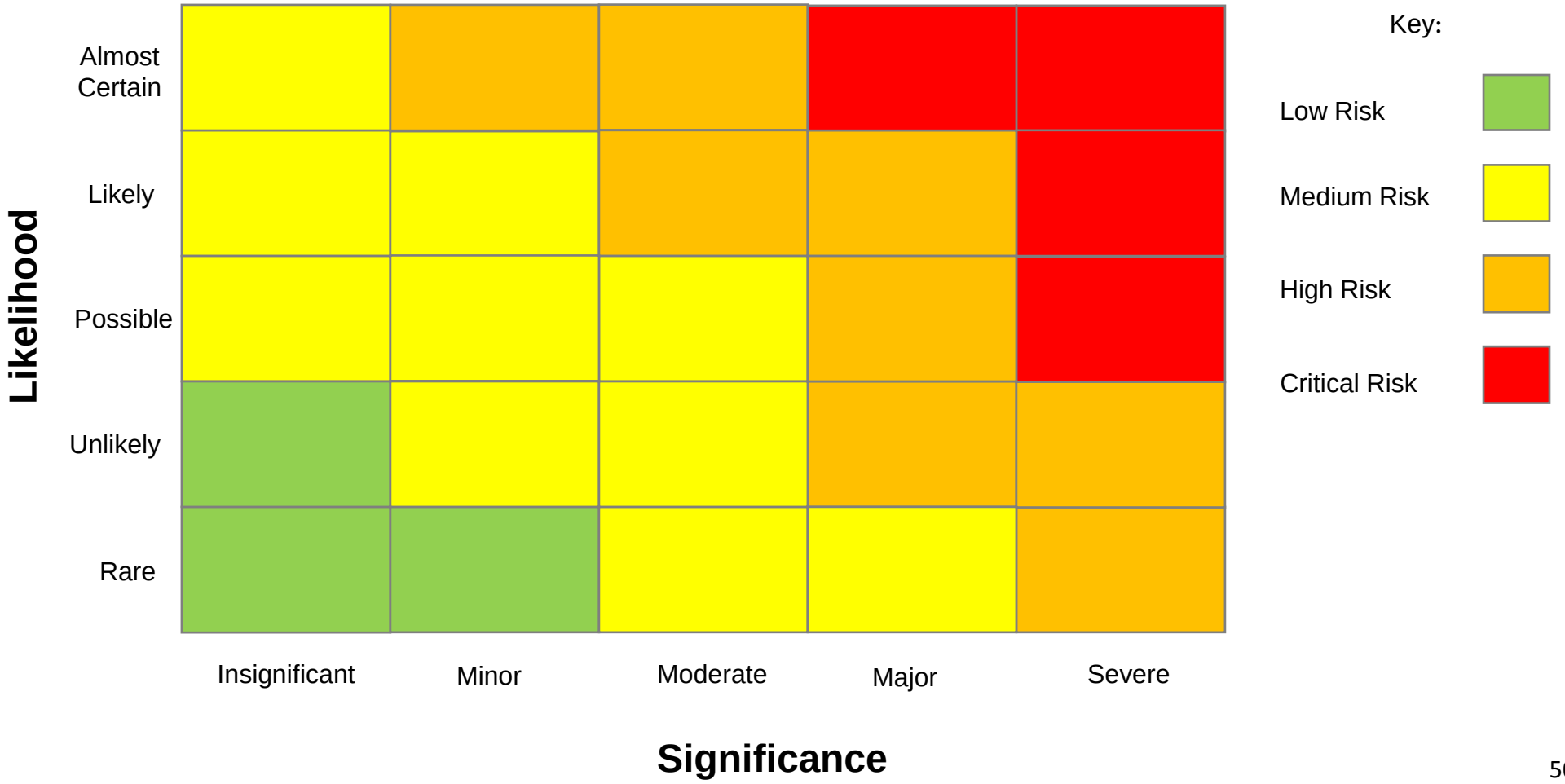


The amount of risk that exists in the absence of controls.

The process or control that the organization puts in place to manage the risk.

The risk that remains after controls have been applied.

Risk Assessment Heat Map



Dynamic Risk Assessment Process

The risk assessment should not be performed solely on an annual basis. Internal Audit should consider the organization's changing environment and how it may impact its risk profile. The dynamic risk assessment process should drive modifications to the audit plan.

- Monitoring Mechanisms:
  - Ongoing meetings with front line units and Risk Management
  - Committee attendance
  - Review of business line assessments and metrics
  - Review of management identified findings and/or findings identified by other testing assurance functions
- Questions to Ask:
  - Has the risk universe changed?
  - Has the audit universe changed?
  - Does the audit plan allow flexibility to respond to these changes?
- Next Steps:
  - Adjust risk assessment to reflect current risk
  - If change in risk drives changes in the audit plan, present necessary changes to the audit plan to the Audit Committee for approval. Communicate risk changes and adjustment to audit plan to front line management and Risk Management, as necessary.

Thank you

Please join us for Q&A following this presentation.