CIBC

CIBC PRIVATE WEALTH

First line of defense – basics

FIRMA breakout session

May 2, 2023

Presented by:
Diana Vasquez, Chief Administrative Officer

Contents

Biography

Diana K. Vasquez

Chief Administrative Officer, CIBC Private Wealth

As the chief administrative officer, Diana Vasquez leads the management and development of our US Private Wealth operating model, ensuring our processes meet the changing requirements of our business. In this role, she acts as an advisor and strategic partner with the firm's client-facing teams to manage the processes and control environment within the business along with the administration and general business management activities. Prior to her current role, Diana was the head of the bank's US governance and controls team, head of risk and administration for CIBC Bank USA, and also previously served as the bank's fiduciary compliance officer within the wealth management department.

Prior to joining the firm, Diana was an attorney in a private practice, where she counseled clients on trust company formation, trust company compliance and estate planning. She was also previously employed at Merrill Lynch Trust Company (now part of Bank of America), where she focused on new business acceptance for the Midwest region and compliance for the trust company.

Diana received a Bachelor of Science in finance and marketing from DePaul University and a Juris Doctor from University of Illinois Chicago School of Law. She is a member of FIRMA and the Chicago Estate Planning Council.

Three lines of defense - an overview

What are the three lines of defense?

First line of defense

- **Management owns the risk** and is accountable and responsible for identifying, measuring, mitigating, monitoring and reporting operational risks
- The first line may use a 1B (control group in first line) to:
  - support overall first line of defense risk management on behalf of first line executive management,
  - conduct independent testing
  - serve as primary executor for first line of defense risk management activities

Second line of defense

- Functionally independent oversight groups with subject matter expertise (risk management, compliance)
- Provides effective challenge

Third line of defense

- Responsible for providing reasonable assurance to senior management and the Audit Committee of the Board of Directors on the effectiveness of the internal controls

Fourth line of defense

- Regulators

Which line of defense do you represent?

Regulatory requirements

Office of the Comptroller of the Currency (OCC)

OCC Comptroller's Handbook: Corporate and Risk Governance, Version 2.0, July 2019

- "Banks should have a risk governance framework commensurate with the sophistication of the bank's operations and business strategies" and these risk governance frameworks vary by banks
- The first line of defense are functions that create risk. These groups are responsible for implementing effective internal controls and maintaining processes for identifying, assessing, controlling, and mitigating the risks associated with their activities consistent with the bank's established risk appetite and risk limits.
- Banks with average total consolidated assets of $50 billion or with greater complexity (i.e., "covered banks") should adhere to 12 CFR Part 30, Appendix D

12 CFR Part 30 Appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks-should include well-defined risk management roles and responsibilities

- **Front line units should assess and effectively manage risks associated with their activities using risk assessments as the basis for fulfilling responsibilities**
- Independent Risk Management (i.e., second line) should oversee the covered bank's risk-taking activities and be accountable to the CEO and board of directors for establishing a risk governance framework and identify and assess on an ongoing basis the material aggregate risks using risk assessments as the basis.
- Internal Audit should maintain inventory of the bank's material processes, product lines, services and functions and establish an audit plan considering the bank's risk profile; and report conclusions to the Board's audit committee.

Regulatory requirements (continued)

Federal Reserve – Large Financial Institutions

12 CFR Parts 211 and 238 effective 2/1/19 Large Financial Institution Rating System

- Applies to holding companies with total consolidated assets of $100 billion or more/US intermediaries of foreign banking organizations under Reg YY with total consolidated assets of $50 billion or more
  - Part of broader initiative by the Fed to develop a supervisory rating system in response to financial crisis
  - Includes ratings for Governance and Controls
    - Effectiveness of board of directors; management of business lines and independent risk management and controls

2018 proposal for core principles of effective senior management, management of business lines: Senior management is responsible for managing the day-to-day operations of the firm and ensuring safety and soundness and compliance with internal policies and procedures, laws, and regulations, including those related to consumer protection

Management of business lines include implementation and execution of strategy and risk tolerance; risk identification and risk management; resources and infrastructure; business controls; accountability

SR 21-3 Supervisory Guidance on Board of Directors' Effectiveness: principles-based approach that provides five attributes of an effective board including: 1) Set clear, aligned and consistent direction regarding firm's strategy and risk appetite; 2) Direct senior management regarding the board's information needs; 3) Oversee and hold senior management accountable; 4) Support the independence and stature of the firm's independent risk management and internal audit functions; 5) Maintain a capable board composition and governance structure

Prudential Standards for Large Bank Holding Companies Savings and Loan Holding Companies, and Foreign Banking Organizations: Standards related to liquidity, risk management and stress testing to reflect risk profile of banking institutions under each category

What is the benefit of a three lines of defense framework?

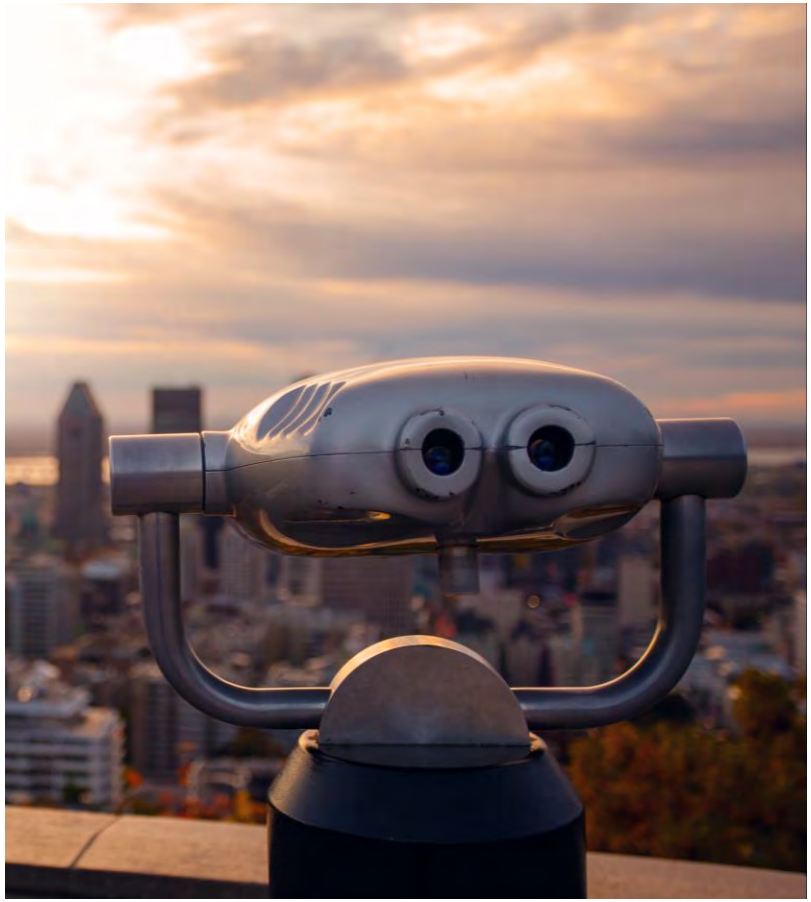
Why should smaller financial institutions consider a three lines of defense framework?

- **Team-based approach to protecting our clients**
- **Allows compliance officer to focus on “bigger” compliance issues**
- **Business unit is closest to the risk- taking activities and is in a better position to identify the risks**
- **Promotes strong risk culture by creating accountability**
- **Gives frontline a voice in policy/procedure creation which would lead to increased compliance**

First line of defense – the details

Front-line Teams (1A) have the primary responsibility to own and manage risks associated with day-to-day operational activities. Client-facing teams and support functions are **the first line of defense** against **challenges** to **the risk standards** that threaten the business and clients.

The **Governance and Controls 1B function will support the front-line** in performing their responsibilities, as needed, help assess risk, monitor certain risk metrics, and support escalation processes.



Key risk activities of the front-line (1A)

- Design, operationalize, and implement controls
- Serve as primary executor of first line of defense risk management activities related to key risk types (e.g., market/liquidity risk, operational risk)

Governance and controls 1B risk activities

How does the 1B facilitate risk management processes on behalf of the business?

Policies, procedures and standards	Support the development, maintenance, and review of business-specific procedures
Risk identification / assessment	Lead and coordinate risk identification activities Work with business to assess inherent & residual operational risk and document mitigation plan Work with business sponsor to assess inherent risk and track mitigation plan for new and change initiatives
Internal control and testing	Work with business to design and implement controls to mitigate risk and conduct management control testing Perform operational and design effectiveness testing on behalf of the business
Issues management	Manage audit; compliance or self-identified findings and assist business in development and implementation of remediation plans
Incident management	Report operational risk incidents to second line and prepare root cause analysis and remediation plan
Metrics	Assist with development of key risk indicators and risk appetite; monitor and report key risk indicators and risk appetite performance to management
Reporting and communication	Design, develop and communicate first line business-level owned reports
Auditor and regulatory support	Act as central point of contact and coordinate internal audit and regulatory review requests and questions
Training	Provide training feedback to Independent Risk Management and review compliance training plans

Identification and assessment of risk

What is the Operational Risk and Control Self-Assessment Process (RCSA)?

- The Risk Self-Assessment is the process by which operational risk exposures are identified and assessed for significant business activities at the process level
- Identifies operational risk; assesses inherent and residual risk and outlines the controls in place to mitigate the risk.

Inherent risk

- A combination of likelihood and impact of a loss prior to applying mitigating controls
- High, medium, low as classified by a taxonomy

Controls

- An activity or procedure that by its effective design and operation would help mitigate the inherent risks within a process (e.g., preventing or detecting an error, material misstatement, a significant operational failure, customer disservice or regulatory non-compliance).
- Control testing and any issues identified are supported by 1B Governance and Control

Residual risk

- The remaining risk after the application of mitigating controls
- High, medium, low more subjective but subject to challenge

Second line responsibilities
Both inherent risk and residual risk are subject to independent challenge by the second line risk associates (consisting of defined subject matter experts for each operational risk type.)

First line responsibilities

- Front-line 1A: Management owns the risk and works with 1B to complete risk assessments
- Governance and Controls 1B: Works with front-line 1A to facilitate risk assessment including identifying key controls and testing and responding to challenge from second line partners

Control and mitigate: Testing example (legal risk)

First line: Ensure ongoing design and operating effectiveness of controls

- **Risk identification:** High inherent risk identified in risk assessment for Inadequate Investment Advisory risk where the organization does not provide advice that matches a client's documented investment objective

- **Controls needed:** Each discretionary account is subject to a Regulation 9 review to assess whether the coded investment objective aligns with the actual holdings in the client's account

- **Control testing example:** Regulation 9 review: Asset allocation
  - Design effectiveness testing is a point in time and could include:
    - Interview personnel
    - Observe the performance of the control
    - Review applicable Regulation 9 procedures
  - Operating effectiveness samples completed investment review to ensure that any asset allocation flags are appropriately addressed through an updated IPS or rebalance of the accounts

Control and mitigate: Testing example (fraud risk)

First line: Ensure ongoing design and operating effectiveness of controls

- **Risk identification:** High inherent risk identified in risk assessment for Account Takeover Risk- email compromise by third party actors (external fraud)

- **Controls needed:** Each money movement request is subject to authentication that includes an independent callback for non-recurring requests

- **Control testing example:** Wire callback process
  - Design effectiveness testing is a point in time and could include:
    - Interview personnel
    - Observe the performance of the control
    - Review applicable authentication procedures
  - Operating effectiveness samples disbursement activity over a period of time to ensure that the client authentication process has been followed

Monitoring and reporting: Key Risk Indicators (KRIs)

First line: Monitor and report KRIs to manage material risk exposure

- Key Risk Indicators (KRI) are a tool that serve as an early warning signal of increasing risk exposures
- Controls are established to prevent or detect risk events and KRIs are based on current activity that allow for forward looking management of risk
- Utilized to prevent the event from occurring
- The early warning is triggered by the metric's proximity to or breach of its established risk tolerance range

---

Example:

Risk event
- Litigation for decline in portfolio market value for concentrated investment
- Operational Risk Type: Legal: advisory activities

Root cause
- Ineffective oversight for off-list/concentrated holdings

KRI
- Accounts holding off-list securities without appropriate rationale (derived through testing)
- Thresholds set by first line on a percentage basis (green amber, red)

Examples of Control Testing Program Coverage

Account setup, maintenance, closing

- Account opening documentation
- Address changes
- Client files and meeting books
- Account closing documentation

Annual administrative and investment reviews

- Quality of Reg. 9 reviews
- IPS review
- Letters of Direction

Fiduciary activities

- Asset transfers
- Distributions (charitable and non-charitable unitrust)
- Discretionary distributions
- wire disbursements
- Unique assets
- Statements

Revenue/fee controls and account oversight

- Fee schedule review
- Final fee form
- Fee set-up

Investments

- Suitability
- Trade errors
- Daily trade review
- Concentration and off-list holdings

Legal and compliance

- Complaints
- Outside business activity
- Third party demands

Office controls

- Disaster recovery – call list
- Secure workspace
- Physical access

Examples of Risk Reporting Content

- **Top and Emerging Risks:** as identified through risk assessments, metric results and open issues.

- **Issues Management:** report can include updates on the number of new issues opened, status of remediation, and root cause analysis. It is also important to show the number of self-identified issues as it can be a measure of an effective risk culture.

- **Control Testing Results:** including updates on the number of new issues opened, status of remediation, and root cause analysis.

Examples of Risk Reporting Content

- **Metric Conformance:** used to identify and monitor risk with different limits and thresholds such as:
  - Early Warning Indicator
  - Management Risk Limit
  - Board Risk Tolerance

  Metric examples:

  - Number of past due/outstanding investment reviews
  - Number of initial new account reviews not completed by due date
  - Failure to perform reporting and processing requirements in accordance with the stated deadlines
  - Inadequate documentation of or failure to follow operating procedures that lead to processing errors or losses
  - Failure to perform reporting and processing requirements in accordance with the stated deadlines

How to avoid common pitfalls

Overlapping roles and responsibilities	Siloed groups within the three lines of defense	Resource constraints
• Clearly document roles and responsibilities across the three lines of defense • Ensure there is adequate training	• Communication and transparency • Sharing of information across three lines of defense	• Adequately staff the first line of defense to execute its responsibilities • Ensure the second line of defense has experience to provide effective challenge

Questions?