As published in ABA Risk and Compliance – July/August 2023

COMPLIANCE FUNDAMENTALS

Understanding the Complexities of Enterprise Risk Management

A Guide for Compliance Professionals

BY SARA MCGINNIS, CRCM, CAMS, CAFP

THE PRUDENTIAL REGULATORS generally define the categories of risk as: credit, interest rate, liquidity, pricing, operational, compliance, strategic, and reputational. These categories are not mutually exclusive, and any product or service may expose a bank to multiple risks. Experience has shown that compliance professionals primarily deal with compliance, legal, and operational risk, but these risks are interrelated. For example, issues with underwriting guidelines may result in credit and compliance/fair lending risk. Daily execution of sales, operations, and servicing activities may result in operational and compliance risks.

Compliance risk is defined as the risk to earnings or capital arising from violations of, or non-conformance with laws, rules and regulations, code of conduct, customer relationship rules or ethical standards. In today's environment, compliance risk remains elevated amidst the creation of new products and services, the increased use of technology for product and service delivery and expanded partnerships with third parties. Compliance risk management is typically integrated into the overall enterprise risk management (ERM) framework of an organization, which involves identifying, assessing, and managing all types of risks across the organization.

The Office of the Comptroller of the Currency (OCC) defines operational risk as the risk of loss resulting from information system failures and business disruptions, human error and fraud, business process and product design defects, and legal challenges. In the ever-changing landscape, operational risk is also increasing as banks face these new challenges. Financial institutions are on a continuing quest to ensure internal controls are in place and operating as intended to address ongoing and emerging compliance and operational issues. Additionally, the complexities of credit, liquidity, pricing, reputational, and strategic risk demand an effective ERM program.

Banks are breaking down the silos between risk management and compliance functions due to increasing complexity in the financial sector and regulatory pressure regarding the need to

understand the importance of a holistic approach to risk management. This integration is driven by the recognition that operational and compliance risk are closely linked - compliance is a risk management discipline, and effective management requires understanding regulatory requirements. Integrating these functions enables banks to manage risk and comply with regulations more efficiently.

Understanding the bank's tolerance or appetite for risk provides the guardrails needed to administer the ERM program and other bank risk programs. These include compliance, fair lending, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), privacy, and information security, to name a few. However, it is also important to identify and assess specific risks across the institution.

Determining the Risk Appetite

Developing methods and controls to deal with risks in all aspects of the business helps an institution prepare for unexpected events while remaining competitive, profitable, and in compliance with regulatory requirements. Risk exists in every institution, however it must be understood and controlled appropriately. As demonstrated by the recent bank failures, effective risk and compliance management are integral to an institution's success.

ERM begins with an understanding of the institution's risk appetite—the level of risk an organization is willing to accept while pursuing its objectives —and before any action is determined to be necessary to reduce the risk. The institution's executive management and board are responsible for establishing tolerance levels, setting the tone for and communicating a risk and compliance-based culture.

Each institution's risk appetite is unique based on a number of factors, such as company culture, competitors, the nature of the objectives pursued, and the financial strength and capabilities of the institution. To facilitate clear communication, the risk appetite should be documented as a statement of acceptable risk tolerances in both qualitative and quantitative terms as illustrated below. The level of detail provided will depend on the bank's preferences and at a minimum should include enterprise-level guidance, with more specific guidance provided within the programs administered under each risk category. For example, for the compliance risk appetite, the compliance policy and program may further detail guidelines and expectations supporting the enterprise risk assessment.

Example—Risk Appetite Statement Excerpts:

Risks	Example Tolerance (Qualitative)	Example Measure (Quantitative)
Credit	Maintain a diversified portfolio that limits high-risk assets.	Portfolio targets: • 40-45% Consumer • 35-40% Commercial and Small Business • 25-30% Commercial Real Estate
Operational	Minimize operational losses through systems of internal controls and monitoring to manage net operational losses (NOL).	Operational loss tolerance threshold • NOL to Net Revenue < .75% is within tolerance • NOL to Net Revenue >1.0% above tolerance
Compliance	ABC Bank requires all employees to comply with the applicable rules, regulations, and policies in the execution of daily activities.	• Effective corrective action on internally identified issues as evidenced by no repeat issues • No Matters Requiring Attention on regulatory examinations

Once risks are understood and tolerance levels established, decisions can be made on which risks will be accepted, hedged, transferred, or mitigated. Actual performance is periodically measured against tolerance levels and reported along with management actions to an executive risk committee and eventually the board of directors. An ERM framework will provide the guardrails for an institution to manage its risk appetite.

ERM Framework and Structure in a Financial Institution

The ERM program outlines the framework to identify and manage all risks within a financial institution. A well-defined framework allows an organization's executive management and board to gain an understanding of exposure areas and provides key data to allow management to mitigate and balance the exposure to ensure coordination of controls and business processes and improve performance. In addition, it can help an institution avoid loss, remain in compliance with regulatory and legal requirements, support growth, and improve profitability.

The ERM framework should be comprehensive, dynamic, and customizable to the institution's size and complexity. It should be configured to include internal risk teams, systems, and processes to continuously monitor the risk universe and provide reports to senior management and the board. A typical framework consists of a board-level risk committee to oversee activities in the areas of corporate responsibility, including compliance, and an audit committee to ensure communication of independent assurance activities to the board.

The Enterprise Approach – Integrated Risk Governance

The ERM framework provides an integrated approach to risk management across the organization that allows management to see the big picture in addition to each risk category. As the institution grows, a senior level enterprise risk management committee (ERMC) helps to oversee and maintain the ERM function. The ERMC is comprised of C-suite executives and provides guidance and effective challenge to identify, measure, monitor, document, remediate, and report on the overall risk environment. Committee minutes are maintained to document effective challenge, support management actions and board reporting.

With so many risks impacting an institution and various departments charged with managing them, it is important to consider how the compliance department interacts and communicates with the other functions and with management. At the most basic level, compliance and other risk professionals should collaborate to provide consistency in the risk terminology used across the organization to avoid confusion. For example, does one department refer to an audit finding, and another area describe an audit issue? Are these the same thing, or is an issue less significant than a finding?

The definitions for issue and report ratings may be customized to the risk function but everyone should understand what a high, moderate, or low rating means. Similarly, key risk and performance indicators (such as the number of open audit findings, or the percentage of defaulted loans) should be described in similar terms throughout the organization.

An institution may benefit from implementing an enterprise governance, risk, and compliance (EGRC) system to centrally organize and manage risk activities and processes. An EGRC system offers an integrated approach that bridges silos and provides insight and transparency into risks across functions facilitating informed business decisions.

Collaboration, communication, and consistency are essential for successful implementation of the ERM program, particularly as the institution grows. Compliance and risk professionals must work together to identify and evaluate how risks impact the whole organization. For example, an

operational error can result in compliance risk. A core system update (operations) that inadvertently changes a fee code resulting in a fee being inaccurately assessed to a segment of customers raises the potential for consumer harm and compliance risk under a specific regulatory requirement and Unfair, Deceptive, or Abusive Acts and Practices (UDAAP).

Importance of Management and Board Reporting

Management and the board must be informed of the results of risk assessments, monitoring, testing, change management, new products and internal audits to ensure operational changes and deficiencies are addressed in a timely manner.

The importance of reporting issues from audit, monitoring and testing, along with appropriate tracking details shouldn't be taken lightly. Examiners focus on the status and remediation of outstanding findings in assessing the effectiveness of ERM programs. Leadership must be well-aware of open issues and corrective action plans. Inadequate issue tracking, resolution procedures and repeat findings may be indicative of larger problems. These could include a lack of clear accountability, an inefficient operating environment or ineffective risk management.

Comprehensive reporting to senior management and the board provides an understanding of the current risk environment along with emerging risks to allow the institution to prepare for unexpected, and potentially unfavorable, events and outcomes.

Closing Thoughts

Understanding ERM is crucial for organizations to identify, assess, and manage risks effectively. By implementing a robust ERM framework that includes compliance risk management, organizations can proactively anticipate and respond to risks that may impact their operations, reputation, and financial performance. A successful ERM program requires the involvement of all stakeholders, including senior leadership, employees, and external partners. With a comprehensive ERM approach in place that also addresses compliance risk, organizations can mitigate risks, capitalize on opportunities, and achieve long-term success.

ABOUT THE AUTHOR

SARA MCGINNIS, CRCM, CAMS, CAFP is a director in the Regulatory Compliance and Internal Audit practice of CrossCheck Compliance LLC. Sara has extensive regulatory compliance and BSA/AML experience having worked in both consulting and industry over the past 25 years. Her expertise includes having managed complex control audits in AML and fraud, risk and control assessments, loan compliance audits, and compliance monitoring reviews. Prior to joining CrossCheck Compliance, she held senior compliance and internal audit positions with U.S. Bank, Associated Banc-Corp, and Johnson Financial Group (WI). She is a past instructor at the Wisconsin Bankers Association Real Estate Lending School and a published author on AML and loan quality control audits. Sara can be reached at smcginnis@crosscheckcompliance.com.

ABA MEMBER RESOURCES

ABA Training: Enterprise Risk Management Reporting: aba.com/training-events/online-training/enterprise-risk-management-reporting

Industry Insight: 5 Steps for Easing into ERM: aba.com/news-research/analysis-guides/5-steps-for-easing-into-erm

Get Certified: Certified Enterprise Risk Professional (CERP): aba.com/training-events/certifications/certified-enterprise-risk-professional