SAI360
RISK FROM EVERY ANGLE

E-book

2023 Bank Failures Spur Proposed Changes

What Risk Managers Need to Know

Background: Setting the Scene

According to the FDIC, bank failures in 2008 and the Spring of 2023 demonstrate institutions with poor corporate governance and risk management practices face a higher risk of failure.

Introduction

In the summer of 2023, the U.S. Federal Reserve and Federal Deposit Insurance Corp. (FDIC) released a proposal that increases the number of banks that would be required to account for unrealized gains and losses. It would also alter the way banks calculate risk-weighted assets.

Public comment on the proposal ended on December 11, 2023, and bank regulators are expected to issue a final ruling later this year.

This e-book discusses the requirements outlined in the proposal, as well as steps financial institutions can take not only to comply if the proposal is adopted, but to also improve their efficiency and broader operational resilience in the process.

Background

This regulation tackles similar challenges related to safety and soundness that smaller Financial Services institutions face, which are regulated by the FDIC rather than the OCC[1]. The OCC, the Office of the Controller of the Currency, is a U.S. federal agency that regulates and supervises national banks and federal savings associations, ensuring their safety, soundness, and compliance with banking laws. They released their Standards in 2014.

Like the OCC Heightened Standards, the new rules would require covered institutions to follow the "three lines of defense approach" to risk management.

The proposed FDIC guidelines, affecting banks with $10b total consolidated assets, will create additional obligations for these institutions to govern. The proposed guidelines are more prescriptive to the board composition, board activities, written policies and the overall risk management process. This will require these organizations, typically less mature from a corporate governance and risk management perspective, to undergo significant change management activities designed to establish and formalize practices that conform to these new obligations with a sustainable program.

1 Office of the Comptroller of the Currency, Federal Register, published September 11, 2014, https://www.occ.gov/news-issuances/federal-register/2014/79fr54518.pdf.

Proposed Guidelines

Increased Board Responsibilities and Guidelines

As a foundational pillar of effective corporate governance, the Board of Directors plays a critical role in steering the organization towards compliance and ethical business practices. The proposed rules introduce new dimensions of responsibility and potential complexity in board oversight processes.

Key aspects include:

- Upholding independent directors to ensure unbiased decision-making and adherence to stricter independence standards
- Board is required to establish appetite statements and the risk profile is to be aggregated and measured quarterly within and across relevant risk categories; for more on this, see page 5
- Setting a clear and ethical tone from the top, which is crucial for fostering a culture of compliance and integrity throughout the organization
- Implementing robust policies for documenting and self-reporting any violations of law, ensuring transparency and accountability
- Regularly reviewing all written policies to maintain relevance and effectiveness in a dynamic regulatory environment
- Broadening the scope of their oversight to consider the interests of all stakeholders, including shareholders, depositors, creditors, customers, regulators, and the public

The proposed guidelines also recommend the establishment of several board committees, each of which emphasizes the separation of internal audit and risk management from “revenue generating” activities. This framework empowers the Board of Directors to navigate the intricacies of governance with a balanced and comprehensive approach, essential for sustaining trust and credibility among all stakeholders.

Key Bank Committees[2]

The chart below provides examples of key committees based on the objectives identified in the proposal.

Audit Committee

ROLE

Oversee financial reporting, audits, internal audit functions.

COMPOSITION

Independent, external directors. Reports progress and necessary actions to full board.

Compensation Committee

ROLE

Ensure compensation doesn't promote risky behavior or legal violations.

FOCUS

Monitor compensation practices, prevent excessive or risky rewards.

Trust Committee

ROLE

Manage risks in trust operations, assure asset separation and compliance.

FUNCTION

Keep trust department distinct and compliant with regulations.

Risk Committee

ROLE

Approve and review risk management policies, oversee risk framework.

REQUIREMENT

Independent director, experienced members. Aligns with banking standards.

2 The guidance further emphasizes that firms should set up additional committees as needed, citing Information Technology/Cybersecurity as a prime example.

Risk Management and Audit: Essential Framework for Financial Institutions

Under the proposed guidelines, the institution should define its risk profile and appetite and establish clear limits. The guidelines would also require the development of a written strategic plan, as well as a written risk appetite statement including both qualitative components and quantitative limits.

Whereas the OCC Heightened Standards prescribes annual reviews, the proposed guidelines would require a quarterly review or more frequent reviews based on the size and volatility of risks faced by the bank.

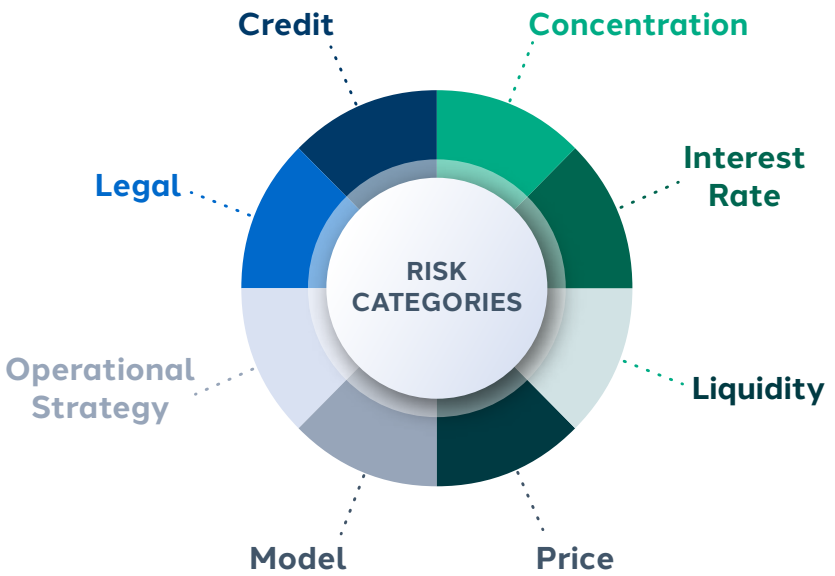
Written Strategic Plan

DEVELOPMENT: Crafted by an independent risk management unit

REVIEW FREQUENCY: Annual reviews and additional assessments during significant risk or business model changes

RISK COVERAGE: The program should address various risk categories

Financial institutions would be required to implement a comprehensive risk management program that encompasses the following key aspects:



Compliance Monitoring and Reporting Structure: Three Roles to Know

Under the proposal, an independent risk management unit would design a formal risk management program. The following three units would be responsible for monitoring and reporting compliance with the program.

1 Business Unit (BU Leader)

RESPONSIBILITIES

Tasked with ensuring their risk-taking activities are confined to those sanctioned by management in accordance with the risk appetite statement

KEY ACTIONS

- Ongoing risk assessment
- Adhere to risk limit policies
- Ensure compliance with board policies
- Quarterly reporting to the risk management unit

2 Independent Risk Management Unit (Led by CRO)

ROLE

Oversee aggregate risks and design risk management program

KEY DUTIES

- Develop risk management program
- Continual material risk assessment
- Monitor risk profile and limit adherence
- Ensure front-line units meet standards
- Supervise front-line units' risk limit compliance
- Report issues to CEO and Risk Committee

3 Internal Audit Unit (Led by CAO)

OBJECTIVES

Ensure compliance with guidelines

KEY FUNCTIONS

- Evaluate risk management policies and processes
- Report on findings and management responses
- Independently assess risk management effectiveness

The Role of GRC Applications

SAI360's Governance, Risk, and Compliance (GRC) platform offers banks a comprehensive framework to address obligations outlined in the proposal.

Governance

Policy Management: SAI360's Policy Management can assist the Board and its committees in reviewing and managing written policies effectively. It offers configurable workflows, version management, and automated alerts, ensuring that policies are up-to-date, compliant, and reflective of stakeholder interests.

Internal Control Enhancement: This feature strengthens the organization's ability to enforce and monitor the effectiveness of its policies. By integrating internal control mechanisms directly into policy management, it ensures compliance with external regulations and adherence to internal standards and procedures.

Frameworks and Business Content: This ensures policies are aligned with industry standards and best practices. it also enhances policy relevance and robustness, addressing unique business challenges and regulatory requirements efficiently.

Issues Management: This is critical for streamlining the identification, tracking, and resolution of policy-related issues. Issues management ensures timely response to challenges, maintaining compliance and operational integrity.

Risk

Integrated GRC Solution: Covers a variety of risk categories and provides a unified view of risk management. The solution's ability to operationalize GRC programs quickly can support the annual review of risks and business model changes.

IT Risk & Cybersecurity: The automation of assessments and enhanced visibility into risks, including IT and cybersecurity, aligns with the Proposed Guidelines' emphasis on operational, IT, and cybersecurity risks.

Audit Management: Empowers audit teams to work more efficiently, providing insights that can assist the Audit Committee in overseeing financial reporting and internal audit functions.

TPRM/BCM Integration: High-level integration with Third-Party Risk Management (TPRM) and Business Continuity Management (BCM) ensures policies are adaptable and resilient, considering external partnerships and continuity strategies. Taken together, they provide a holistic view of risks and preparedness.

Compliance

Incident Management: The ability of SAI360's Incident Management to manage and automate the incident response lifecycle, including documenting evidence and evaluating root causes, is crucial for compliance with the Proposed Guidelines. This feature aids in handling breaches to risk limits and violations of laws or regulations.

Regulatory Change: Featuring an intuitive workflow and augmented regulatory content, Regulatory Change Management helps banks stay compliant with evolving regulations and the Proposed Guidelines. This tool is especially relevant given the dynamic nature of regulatory standards.

Conflicts of Interest Management: With a dedicated focus on managing conflicts of interest, COI Management ensures policies are in place to effectively identify, mitigate, and manage potential conflicts. This helps maintain high ethical standards and organizational integrity.

Exam Management: Efficiently prepare for and manage regulatory exams, reducing the burden on compliance teams and ensuring compliance with applicable regulations. Provide visibility into upcoming exams and related details in an exam calendar.

Obligations Management: This ensures regulatory, legal, and ethical obligations are clearly identified, tracked, and integrated into policy development and updates. This also ensures compliance and reduces the risk of breaches.

Consequences

Because the Proposed Guidelines incorporate a level of prescriptive detail, the FDIC would have more avenues to take enforcement action against a bank for corporate governance and risk management deficiencies identified during examinations.

Like the OCC'S heightened standards, the FDIC's Proposed Guidelines[3] are based on Section 39 of the Federal Deposit Insurance Act, which allow the relevant agency to bring an enforcement action in federal district court and may seek a civil money penalty for each day of the violation. What is the "economic impact" of the regulation? There is added regulatory burden, estimated by the FDIC, to be approximately 91,135 hours annually. This equates to an estimated cost of around $14 million, contingent on staffing expenses.

3 Federal Deposit Insurance Corporation, "Proposed Rules," October 11, 2023, https://www.fdic.gov/news/board-matters/2023/2023-10-03-notational-fr.pdf.

Two SAI360 Case Studies

An Integrated GRC Solution to Manage Operational Risk, Internal Control and Compliance with SAI360

SUMMARY: A bank, which wishes to remain anonymous, implemented SAI360's integrated solution to unify operational risk, internal audit, and compliance processes, replacing separate legacy systems and manual spreadsheets. The solution provided a real-time, holistic view of non-financial risks across the bank, enhancing risk management and promoting efficiency through a centralized data source and systematic issue tracking. This initiative has led to greater transparency, improved oversight, and ongoing upgrades for functionality, supporting continuous improvement in the bank's risk and control performance.

Banking on GRC Success with SAI360

SUMMARY: Robeco, a global asset management firm, implemented SAI360 to address its need for an integrated GRC solution, meeting compliance requirements like Basel II and Sarbanes-Oxley while supporting process and risk management. The SAI360 GRC platform provided Robeco with enhanced visibility into its financial data, business processes, risks, and controls, enabling effective and standardized risk management across the organization. This solution has facilitated enterprise-wide convergence of governance, risk, and compliance, ensuring Robeco's adherence to international regulations and aiding in the development of a comprehensive, scalable control framework.

Want to learn more about how SAI360 is helping financial institutions manage their governance, risk and compliance obligations?

Let's start a conversation. Schedule a virtual coffee with a team member.

Click here to demo our GRC solutions.

This e-book was made possible through contributions from the SAI360 team, along with the support of Scott Cogan and Shimon Ganz, both Senior Vice Presidents of Sales at SAI360.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination