Banking

The banking industry has been the starting point for regulators’ intensified focus on operational integrity and operational risk, generating a vast array of regulations and guidance that are shaping similar efforts in other sectors.

Heightened expectations issued by the Office of the Comptroller of the Currency (OCC) have been replaced with heightened standards that provide more explicit guidance on how major banks should manage risk. These standards are particularly challenging for US affiliates of global banks, which must comply with guidance both from US and global regulators—guidance that is sometimes conflicting or redundant.

In the US, the Federal Reserve Bank (Fed) has overarching responsibility for managing risk in the banking industry. To that end, the Fed is looking for banks to adopt a more coordinated, top-down approach to operational integrity and risk management. In the past, it was common for banks to allow each part of the business to manage risk on its own. But now major banks are expected to manage risk in a more comprehensive and coordinated manner, using governance structures that span the entire global enterprise.

Here are some key regulations and regulatory guidance shaping operational integrity in the banking industry:


Under these guidelines, a covered bank must establish and implement a written risk governance framework to manage and control all types of risk: credit risk, interest rate risk, liquidity risk, price risk, operational risk, compliance risk, strategic risk, and reputation risk. The framework is to be reviewed and updated by independent risk management on an annual basis, or more frequently if needed, to address improvements in industry risk management practices and changes in the covered bank’s risk profile. The guidelines also outline minimum standards for a covered bank’s board of directors to provide oversight of the risk governance framework’s design and implementation.

Key required features of the risk governance framework:

- **Clearly defined roles and responsibilities**: Front-line units, independent risk management, and internal audit (three lines of defense).
- **Strategic plan**: Each covered bank must, at minimum, prepare a three-year plan that comprehensively assesses the risks that could have a major impact on the business during the period. Also, the plan must be evaluated and approved by the board of directors at least annually.
- **Risk appetite statement**: A covered bank should have a comprehensive written risk appetite statement that serves as the basis for the risk governance framework and includes both qualitative components (that describe a safe and sound risk culture) and quantitative limits (that incorporate sound stress testing processes, as appropriate, and that address the covered bank’s earnings, capital, and liquidity).

Other banking regulators have developed their own detailed guidance in more focused risk areas, including the area of operational integrity.

**Code of Federal Regulations Title 12: Chapter 1: Part 30 (12CFR 30) Appendix B: Guidelines from the OCC on information security standards**

These guidelines apply to customer information maintained by (or on behalf of) financial institutions over which the OCC has authority, providing standards for “developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information,” as well as “the proper disposal of consumer information.”

Note that since information security is an interagency issue, there are nearly identical regulations from the Federal Reserve Board (12CFR part 208: Appendix D-2 and part 225: Appendix F) and from the FDIC (12CFR 30 part 364: Appendix B).

Companies are expected to assess, manage, and control information security risks—including risks associated with their third-party service providers. Specific objectives are to: “ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and ensure the proper disposal of customer information and consumer information.”

The guidelines also describe response programs and customer notification procedures that financial institutions should develop and implement to address unauthorized access to (or use of) customer information that could result in substantial harm or inconvenience to a customer.
Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool

In response to the increasing volume and sophistication of cyber threats, the FFIEC developed a tool to help institutions identify their risks and determine their cybersecurity preparedness. The assessment tool incorporates cybersecurity-related principles from the FFIEC Information Technology (IT) Examination Handbook and regulatory guidance, as well as concepts from other industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Key focus areas and benefits include:

- Identifying factors contributing to and determining the institution’s overall cyber risk.
- Assessing the institution’s cybersecurity preparedness.
- Evaluating whether the institution’s cybersecurity preparedness is aligned with its risks.
- Determining risk management practices and controls that are needed, or that need to be improved—along with the actions to be taken to achieve the desired state.
- Informing risk management strategies.

Also, this tool can help organizations assess and track their cybersecurity preparedness over time.

Managing third-party operational risk

According to OCC bulletin 2013-29, which provides guidance on risk management related to third-party relationships, banks continue to increase the number and complexity of activities and relationships with both foreign and domestic third parties, including:

- Outsourcing entire bank functions to third parties, such as tax, legal, audit, or information technology operations.
- Outsourcing lines of business or products.
- Relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the bank’s operations.
- Working with third parties that engage directly with customers.
- Contracting with third parties that subcontract activities to other foreign and domestic providers.
- Contracting with third parties whose employees, facilities, and subcontractors may be geographically concentrated.
- Working with a third party to address deficiencies in bank operations or in compliance with laws or regulations.

Given the growing volume and complexity of third-party relationships in banking, the OCC is concerned that the quality of risk management over third parties may not be keeping pace. According to the OCC, a bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships. Key features of such a process include:

- Plans that outline the bank’s strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
- Proper due diligence in selecting a third party.
- Written contracts that outline the rights and responsibilities of all parties.
- Ongoing monitoring of the third-party’s activities and performance.
- Contingency plans for terminating the relationship in an effective manner.
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process.
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
- Independent reviews that allow bank management to determine that the bank’s process aligns with its strategy and effectively manages risks.
Various privacy laws

The Gramm-Leach-Bliley Act (GLBA), which was signed into law on November 12, 1999, enacted new privacy-related provisions for financial institutions and authorized federal agencies to adopt regulations to implement the new provisions as well as pre-existing provisions of the Fair Credit Reporting Act (FCRA). The financial institutions covered by the GLBA included national banks and their financial and operating subsidiaries, as well as a wide range of other businesses engaged in financial-related activities.

Although GLBA was enacted more than 15 years ago, it continues to serve as the foundation for privacy-related regulations in financial services. Its three principal requirements relating to the privacy of consumer financial information are:

• Financial institutions must provide their customers with notices describing their privacy policies and practices, including their policies with respect to the disclosure of non-public personal information to their affiliates and to nonaffiliated third parties. The notices must be provided at the time the customer relationship is established and annually thereafter.

• Subject to specified exceptions, financial institutions may not disclose nonpublic personal information about consumers to any non-affiliated third party unless consumers are given a reasonable opportunity to direct that such information not be shared (i.e., to opt out).

• Financial institutions generally may not disclose customer account numbers to any non-affiliated third party for marketing purposes.6

While the GLBA is the most extensive federal financial privacy law, there are a number of other statutes that affect information-sharing practices in financial services, including:

• The Electronic Fund Transfer Act protects individual consumers engaging in electronic fund transfers, which include transfers through automated teller machines, point-of-sale terminals, automated clearinghouse systems, remote banking programs, and telephone bill-payment plans in which periodic or recurring transfers are contemplated.7

• The Right to Financial Privacy Act was enacted to provide the financial records of financial institution customers a reasonable amount of privacy from federal government scrutiny. Prior to passage of the act, bank customers were not informed that their personal financial records were being turned over to a government authority and could not challenge government access to the records.8

• The Children’s Online Privacy Protection Act covers online collection of personal information from children under age 13. The act spells out the responsibilities of website operators regarding children’s online safety and privacy. Financial institutions that operate a website or online service directed to children fall under this regulation.9

These laws are currently in effect, and national banks and their subsidiaries are expected to fully comply with them, as well as with any applicable state privacy laws.
Contacts

Chris Spoth
Executive Director
Deloitte Center for Regulatory Strategy
Deloitte & Touche LLP
cspoth@deloitte.com

Dave Wilson
Independent Senior Advisor to Deloitte & Touche LLP
daviwilson@deloitte.com

Endnotes
2. Code of Federal Regulations (CFR), Title 12, Chapter I, Part 30—Safety and soundness standards
4. FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors, FFIEC
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.