Deloitte.

Operational integrity enhancement

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

In the past, regulators did not exert much influence over a company's information systems as long as those systems operated within reasonable standards of safety, soundness, and security. However, that traditional approach to IT regulation is now starting to change. In today's increasingly digital and data-driven world, information systems and data play a crucial role—not only in business, but also in our personal lives and society as a whole. In fact, many of our society's fundamental pillars—such as our financial markets, communication networks, and power grid—would be completely inoperable without reliable information systems that do what they are supposed to do.

For example, if a securities firm's trading systems misfire, the potential negative impact is no longer limited to a few bad trades. Rather, there is now a very real possibility that such a problem could trigger a far-reaching chain reaction that crashes investment markets, undermines our financial system, and perhaps even cripples the global economy.

This large and growing potential for widespread damage from information system problems is prompting regulators in major industries to establish increasingly strict requirements and detailed guidance on how companies manage their IT systems and data. Regulators are particularly concerned about problems that could:

- Prevent critical markets and infrastructure from functioning properly.
- Threaten the health and survival of entities that are essential to our financial system and way of life.
- Compromise customer data and put citizens at risk.

Operational integrity defined

To try and avoid such problems, regulators are taking active steps to help ensure the "operational integrity" of the companies they oversee. From a company's perspective, this means:

> ***Having systems, processes, and people that do what they are supposed to do—effectively, accurately, reliably, and securely—with the resilience to withstand threats and bounce back quickly from problems, no matter how severe.***

This direct supervisory oversight of system integrity, security, and resilience within a business—which can be quite detailed and, at times, even prescriptive—is a major departure from regulators' traditional arms-length approaches to operational and IT risk management. In effect, it imposes a rigorous testing and supervisory process to help ensure that companies are following appropriate processes and procedures; that they can identify and mitigate risks in a timely manner; and that they have sufficient controls in place to ensure a high level of system integrity, security, and resilience.

Specific objectives that regulators have for the companies they oversee include:

- Developing processes, procedures, and controls to help ensure systems do what they are supposed to do.
- Safeguarding systems from internal and external threats (including cyber threats).
- Developing processes and procedures to quickly respond to problems and proactively mitigate risks.

In some cases, regulators' recommendations and guidance are presented as optional. However, in practice, they are effectively requirements because a company that ignores them opens itself up to criticism. And if problems arise, company leaders may have a hard time claiming they acted with sufficient due diligence. Also, while the required testing is often technically limited to critical systems that perform critical business functions, in practice the requirement often extends to include all critical systems throughout the enterprise.

Note that "operational integrity" as defined here is somewhat different from other similar-sounding terms used by various industries—although there may be some overlap in scope. For example, a key focus for banking regulators is "operational risk," which sounds a lot like "operational integrity," and covers some of the same ground. But it also addresses issues that are beyond the scope of operational integrity, such as requiring banks to hold a certain amount of capital to protect themselves from catastrophic losses.

In the future, it might make sense for companies to manage operational integrity as one element in a broader framework for managing all major risks across the enterprise—including how employees conduct themselves. But, for now, the immediate challenge is for companies to address the issue of information-system integrity, security, and resilience.

Regulatory scope

Emerging regulations and regulatory guidance related to operational integrity cover each step of the information system lifecycle:

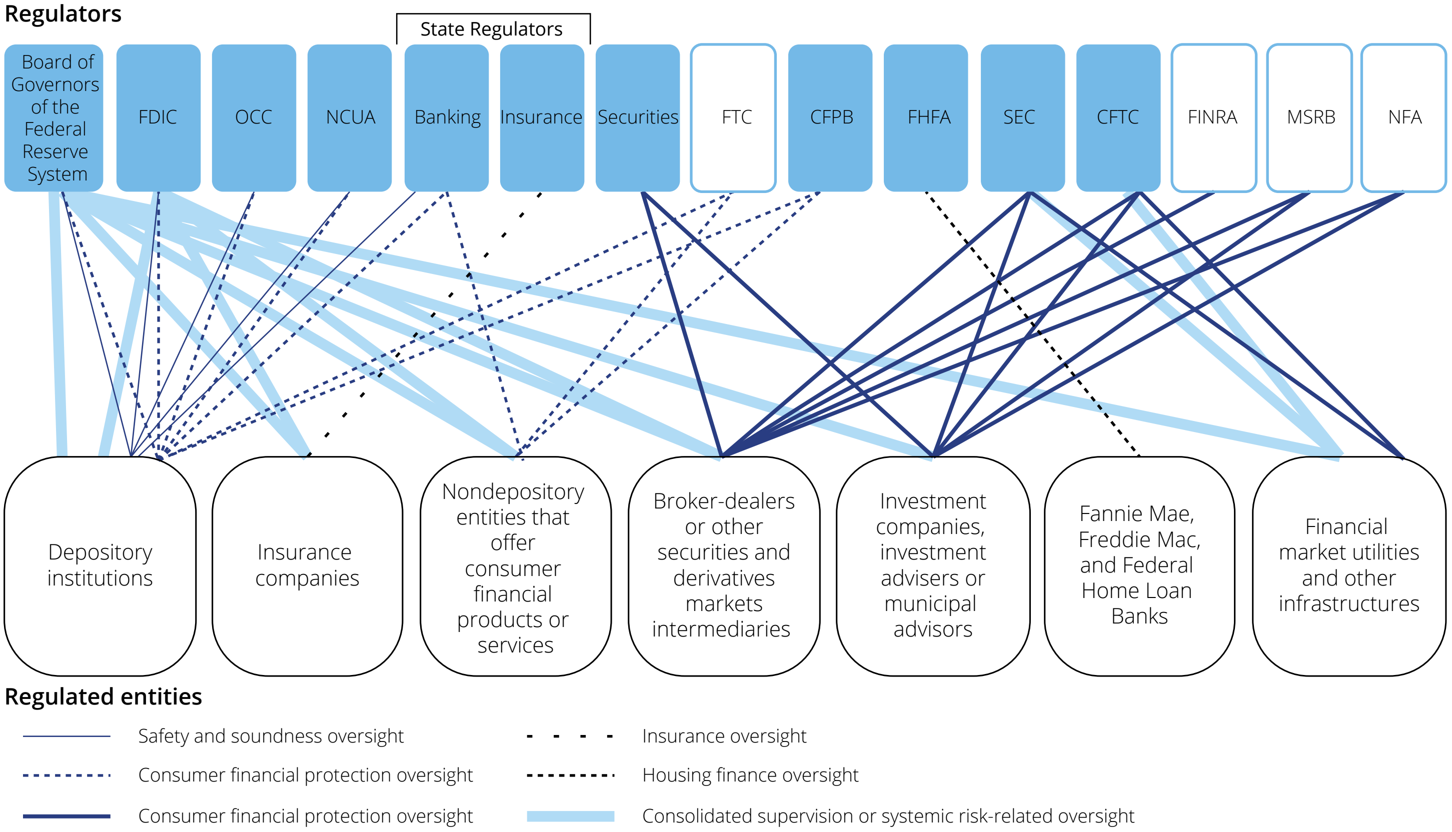
- **Development.** Ensuring a system is properly designed to do what it is supposed to do, with supporting documentation as evidence.
- **Pre-production testing.** Making sure the system functions as designed, in accordance with applicable rules and regulations.
- **Implementation.** Rolling out the system using a robust change management framework that helps ensure people use it correctly.
- **Operation and monitoring.** Monitoring the system to ensure it is operating correctly and doing what it should. Also, monitoring for a wide range of risks and threats, from data breaches and cyberattacks to system capacity and the impact the system is having on external markets and societal infrastructure.
- **Governance.** Having effective internal governance over systemically critical systems, using a formal governance framework that clearly defines roles and responsibilities (i.e., three lines of defense) and helps ensure the proper procedures and processes are being followed.
- **Remediation.** Having a clearly defined path and process for escalating problems to a management level where timely remediation can occur. Also, having clear processes and procedures for handling critical risks, such as how to notify customers in the event of a data breach.
- **Effectiveness testing.** Ensuring that the system is operating effectively and doing what is supposed to do—meeting the needs of internal and external customers and users—while complying with applicable rules and regulations.

Redundant and conflicting regulations and guidance

One of the biggest challenges for companies trying to satisfy the regulatory expectations for operational integrity is the sheer number of entities generating regulations and guidance—much of which is redundant or conflicting. No regulators want to appear lax in this critical area, so they are all tackling the problem aggressively—often without coordinating their efforts.

Within a given industry, sometimes there is coordination between regulators and sometimes there isn't. However, across industries, there is generally little or no coordination among regulators, even when the industries are similar and closely related. For example, in the financial services sector, regulators in various sub-sectors—such as banking, securities, and insurance—are all independently generating their own requirements and guidance for operational integrity. This is a major problem for financial services companies, since many are involved in multiple sub-sectors and must therefore somehow reconcile all of the conflicts and redundancies in order to develop workable solutions.

Figure 1: US financial regulatory structure, 2016[1]


Regulators
State Regulators
Board of Governors of the Federal Reserve System
FDIC
OCC
NCUA
Banking
Insurance
Securities
FTC
CFPB
FHFA
SEC
CFTC
FINRA
MSRB
NFA
Depository institutions
Insurance companies
Nondepository entities that offer consumer financial products or services
Broker-dealers or other securities and derivatives markets intermediaries
Investment companies, investment advisers or municipal advisors
Fannie Mae, Freddie Mac, and Federal Home Loan Banks
Financial market utilities and other infrastructures
Regulated entities
Safety and soundness oversight
Consumer financial protection oversight
Consumer financial protection oversight
Insurance oversight
Housing finance oversight
Consolidated supervision or systemic risk-related oversight

CFBB	Bureau of Consumer Financial Protection
CFTC	Commodity Futures Trading Commission
FDIC	Federal Deposit insurance Corporation
FHFA	Federal Housing Finance Agency
FINRA	Financial Industry Regulatory Authority
FTC	Federal Trade Commission
MSRB	Municipal Securities Rulemaking Board
NCUA	National Credit Union Administration
NFA	National Futures Association
OCC	Office of the comptroller of the Currency
SEC	Securities and Exchange Commission

🟦 Financial Stability Oversight council member agency

Source: GAO. | GAO-18-175

Note: This figure depicts the primary regulators in the U.S. financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure.

The challenge is even greater for multinational companies since they must comply with requirements and guidance from local regulators in all jurisdictions in which they operate, as well as from global regulatory bodies.

Industry overview

The risks related to inadequate operational integrity are most evident in our financial system, where "flash crashes" and other headline-grabbing problems have exposed just how deeply today's society relies on information systems—and how vulnerable we are to system integrity issues. As a result, much of the regulatory activity that has taken place to date around operational integrity has centered on banking, securities, and investment management—especially banking, in light of experiences from the financial downturn.

In recent years, there have been widespread reforms to help ensure banks have the strength and resilience to avoid and survive future crises without government intervention. These reforms affect all aspects of the banking business, from increased capital requirements and financial stress tests to restrictions on what banks can invest in and how multinational banks are structured. The reforms also include detailed regulations and regulatory guidance about how critical information systems are designed, tested, operated, monitored, and governed—a set of activities that matches our definition of "operational integrity."

Operational integrity regulations and guidance developed for the banking industry have inspired similar regulations and guidance for the securities industry. And both of those industries are inspiring similar efforts in insurance, although the insurance industry is not as far along, with specific regulations and guidance still being developed. Operational integrity is also an emerging and important focus for many other industries, including energy and life sciences, all of which are addressing the issue in different ways and are at different levels of regulatory maturity. The appendix of this document provides a closer look at operational integrity regulations, guidance, and trends for individual industries.

Major improvement opportunities

Although every industry is somewhat different when it comes to operational integrity, many of the requirements and challenges they face are fundamentally the same. Here are some important improvement opportunities that companies in all industries can use to help satisfy the demands for more robust operational integrity:

- **Top-down and bottom-up risk management.** More and more C-suite executives are recognizing the importance of operational integrity and are driving efforts and governance from the top down. However, many companies lack bottom-up controls with sufficient granularity to identify and address critical risks. Effective operational integrity requires both.

- **Business ownership of IT risks.** Operational integrity is a strategic business issue, not just an IT issue. Companies need improved transparency so the business can supervise how information systems are developed and managed, rather than leaving it to IT. Business executives must have a clear view of the risks and accurate information about whether those risks are being managed effectively.

- **Coordinated solutions to uncoordinated requirements.** In response to the complex and often redundant or conflicting guidance from various regulators, companies need to develop practical solutions and approaches that feature common controls, common processes, and common systems to assess and address risk across the enterprise—all under the oversight of common governance.

- **Better documentation of functional requirements to support testing.** Operational integrity starts with clear and thorough documentation about what a system is supposed to do. This is critical to the design process, and also provides essential input for testing.

- **Processes and tools to protect customer information and deal with breaches.** Companies need to make a conscious effort to protect customer data, supported by formal guidelines and other mechanisms. They also need to develop clear processes and procedures in advance for dealing with breaches, instead of reacting on-the-fly after a problem occurs.

- **Solutions that address the issue of third-party risk.** In a business environment where companies are increasingly disaggregated and reliant on business ecosystems, managing third-party risk (risks within your value chain partners and service providers) is just as important as managing risk within the four walls of the business.

- **Develop and document a risk assessment process.** The process should clearly define how risks will be identified, prioritized, and addressed—and what controls will be used to monitor those risks.

- **Culture shift.** Operational integrity cannot be achieved solely through new systems and processes; ultimately it relies on employee behavior and organization. Companies need to make sure people are actually following the procedures. This requires educating and training business owners—as well as professionals in compliance and legal—about the importance of IT controls. Perhaps even more important, it requires a culture of compliance in which people throughout the organization have a natural tendency to do what they are supposed to do.

The first step to achieving operational integrity is to clearly understand the general regulatory trends and your company's specific responsibilities. The next step is to perform a comprehensive review of your IT risk program to ensure that management can fulfill its supervisory obligations in overseeing the development and operation of systems used in the business. This includes a review of the IT governance structure, as well as the establishment of policies and procedures to ensure industry-leading practices are in place for all critical systems—including systems operated by third-party vendors—that could cause harm to your customers and your financial viability, as well as to societal pillars such as the financial markets.

Companies today should ensure that adequate processes and tools are in place for monitoring, testing, and reporting, such that management can adequately assess the overall level of systemic risk and determine if the company's IT controls are being properly enforced.

Ready. Set. Go.

Companies wrestling with the challenge of operational integrity face complexity from all angles, including conflicting and redundant guidance and requirements from a variety of regulators. To develop workable solutions, companies must reconcile and rationalize all of that diverse guidance into a unified vision and approach. Rigorous testing is also key.

Unfortunately, most companies won't get serious about operational integrity until regulators start formalizing requirements and dishing out fines. And by then it might be too late. Problems related to operational integrity already pose a very real threat to company reputations and well-being—and may even threaten a company's survival. Also, operational integrity is critical to the health and integrity of our financial markets—and our society as a whole. As such, operational integrity is a challenge that needs to be addressed immediately. Now is the time to get started.

Contacts

Securities

Susan Ameel
Managing Director
Deloitte Advisory
Deloitte & Touche LLP
sameel@deloitte.com

Mike Jamroz
Partner
Deloitte Advisory
Deloitte & Touche LLP
mjamroz@deloitte.com

Banking

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

Energy

Mike Prokop
Managing Director
Deloitte Advisory
Deloitte & Touche LLP
Mprokop@deloitte.com

Insurance

Howard Mills
Managing Director
Deloitte Advisory
Deloitte & Touche LLP
howmils@deloitte.com

The Center wishes to thank the following Deloitte professionals for their insights, support, and contributions to the report:

Zach Dressander, senior marketing specialist, Deloitte Center for Regulatory Strategy, Deloitte Services LP
Shari Gribbin, Deloitte Advisory senior manager, Deloitte & Touche LLP
David Haas, Deloitte Advisory senior manager, Deloitte & Touche LLP
Lara Hamilton, Deloitte Advisory senior manager, Deloitte Center for Regulatory Strategy, Deloitte & Touche LLP
Alex LePore, Deloitte Advisory senior consultant, Deloitte & Touche LLP

Endnotes

[1] http://www.gao.gov/products/GAO-16-175

CENTER *for*
REGULATORY STRATEGY
AMERICAS

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.

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.