Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2019

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation
Office of Inspector General

Date: February 14, 2019

Memorandum To: Board of Directors

From: Jay N. Lerner
Inspector General

Subject Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

I am attaching to this memorandum the Office of Inspector General's annual assessment of the Top Management and Performance Challenges facing the Federal Deposit Insurance Corporation (FDIC). We identified these Challenges based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private sector entities. We considered this body of information in light of the current operating environment and circumstances, as well as our independent judgment.

The FDIC plays a critical role in maintaining the stability of our financial system, and in protecting the savings of millions of Americans. It insures more than $7.4 trillion in deposits at more than 5,400 financial institutions, and directly supervises about 3,500 of these banks. The FDIC also oversees the resolution and receivership of failed banks, consumer financial protection, and management of the Deposit Insurance Fund. Therefore, it is important to address these complex Challenges facing the agency.

The FDIC faces Challenges in several critical areas, a number of which remain from previous years:

- Enhancing Oversight of Banks' Cybersecurity Risk;
- Adapting to Financial Technology Innovation;
- Strengthening FDIC Information Security Management;
- Preparing for Crises;
- Maturing Enterprise Risk Management;
- Sharing Threat Information with Banks and Examiners;
- Managing Human Capital;
- Administering the Acquisitions Process; and
- Improving Measurement of Regulatory Costs and Benefits.

We note that these Challenges will require constant attention and vigilance by the FDIC for the foreseeable future. We anticipate that this document will be informative for policymakers, including the FDIC and Congressional oversight bodies. We hope that it will also be instructive for the American people to learn about the operations at the FDIC and better understand the Challenges it confronts.

Attachment

INTRODUCTION

Each year, Federal Inspectors General are required to identify and report on the top challenges facing their respective agencies, pursuant to the Reports Consolidation Act of 2000. The Office of Inspector General (OIG) is therefore issuing this report, which identifies the Top Management and Performance Challenges (TMPC) facing the Federal Deposit Insurance Corporation (FDIC).

This TMPC report is based upon the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from Government agencies and officials, and information from private-sector entities. We considered this body of information in light of the current operating environment and circumstances and our independent judgment.

The FDIC faces Challenges in several critical areas, a number of which remain from previous years:

- Enhancing Oversight of Banks' Cybersecurity Risk;
- Adapting to Financial Technology Innovation;
- Strengthening FDIC Information Security Management;
- Preparing for Crises;
- Maturing Enterprise Risk Management;
- Sharing Threat Information with Banks and Examiners;
- Managing Human Capital;
- Administering the Acquisitions Process; and
- Improving Measurement of Regulatory Costs and Benefits.

We believe that the FDIC should focus its attention on these Challenges, and we hope that this document informs policymakers, including the FDIC and Congressional oversight bodies, and the American public about the programs and operations at the FDIC and the Challenges it faces.

1 | ENHANCING OVERSIGHT OF BANKS' CYBERSECURITY RISK

Cybersecurity continues to be a critical risk facing the financial sector. Cyber risks can affect the safety and soundness of institutions and lead to the failure of banks, thus causing losses to the FDIC's Deposit Insurance Fund. For example, a cybersecurity incident could disrupt services at a bank, resulting in the exploitation of personal information in fraudulent or other illicit schemes, and an incident could start a contagion that spreads through established interconnected banking relationships. Despite increased spending on cybersecurity, banks are encountering difficulties in getting ahead of the increased frequency and sophistication of cyberattacks. The FDIC's information technology (IT) examinations should ensure strong management practices within financial institutions and at their service providers.

According to the Group of 7 industrialized countries, "cybersecurity risks to the global financial system are of critical concern," and attacks in cyberspace are "increasing in sophistication, frequency, and persistence, cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems."[1] The Office of the Comptroller of the Currency (OCC) echoed this sentiment in its *Semiannual Risk Perspective* (Fall 2018), finding that cybersecurity threats "target operational vulnerabilities that could expose large quantities of personally identifiable information and proprietary intellectual property, facilitate misappropriation of funds and data at the retail and wholesale levels, corrupt information, and disrupt business activities."[2] The Financial Stability Oversight Council (FSOC) similarly recognized in its 2018 Annual Report that as financial institutions increase their reliance on technology, there is an increased risk that a cybersecurity event could have "severe negative consequences, potentially entailing systemic implications for the financial sector and the U.S. economy."[3]

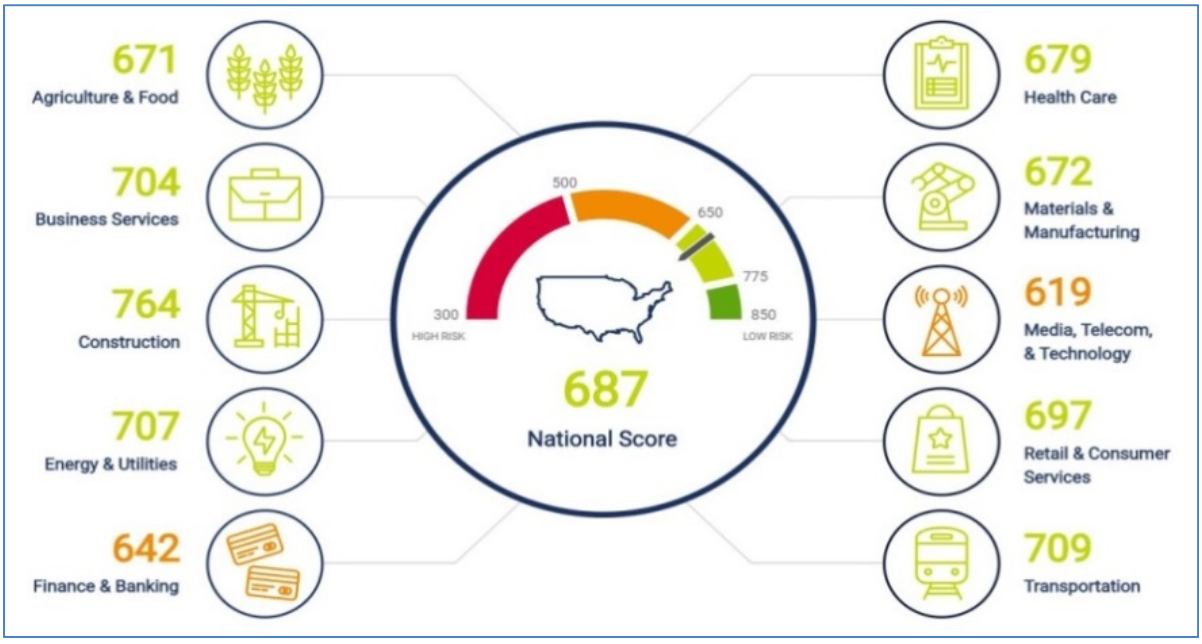
In February 2018, the White House Council of Economic Advisors estimated that the United States economy loses between $57 and $109 billion per year to malicious cyber activity. Cyberattacks—such as distributed denial of service and ransomware—may be global in nature and have disrupted financial services in several countries around the world.[4] Verizon Communications conducted its annual review of global data breaches across multiple sectors, including the financial sector, and reported that there were more than 53,000 security incidents and 2,200 data breaches across 65 countries between April 2017 and April 2018.[5] This review also found that these cyberattacks happen very quickly, and often surreptitiously; nearly

[1] Group of 7, *Fundamental Elements of Cybersecurity for the Financial Sector*, (October 2016). The Group of 7—Canada, France, Germany, Italy, Japan, The United Kingdom, and the United States— meet annually to discuss issues of global economic governance.
[2] OCC *Semiannual Risk Perspective*, (Fall 2018), 16.
[3] The *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010* established the FSOC, which has responsibility for identifying risks and responding to emerging threats to financial stability. The FSOC brings together the expertise of Federal financial regulators (including the FDIC), an independent insurance expert, and state regulators.
[4] World Bank Group, *Financial Sector's Cybersecurity: Regulations and Supervision* (2018), 1.
[5] Verizon Communications Inc., *2018 Verizon Communications Data Breach Investigations Report*, 11th Edition (April 2018).

90 percent of the reported breaches occurred within seconds, and about 70 percent went undiscovered for months.

The American Bankers Association also noted that "as businesses ramp up their cybersecurity efforts, threat vectors such as ransomware have become more frequent and potent, affecting companies in nearly every sector and posing significant risk to financial institutions."[6] One study by the U.S. Chamber of Commerce and FICO (Fair Isaac Corporation) evaluated the cyber risk at 2,574 U.S. firms across ten sectors, including the financial sector. This study provided cybersecurity ranking scores from 300 (high risk) to 850 (low risk) for each sector as well as a national average. The cyber risks faced by the finance and banking sector exceeded eight other sectors and the national average, as shown in Figure 1.

Figure 1: Cyber Risk Scores Across Ten Sectors



Source: U.S. Chamber of Commerce and FICO, *Assessment of Business Cybersecurity* (Q4 2018).

IT Examination Programs and Resources

The FDIC Rules and Regulations, Part 364, Appendix B contains *Interagency Guidelines Establishing Information Security Standards* for bank regulators that state that an insured financial institution must "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities."[7] The FDIC and other regulators conduct IT examinations using the Uniform Rating System for Information

[6] American Bankers Association Journal, *Top Bank Risks in 2018* (December 11, 2017).
[7] 12 C.F.R. Part 364, Appendix B. The FDIC, OCC, and Board of Governors of the Federal Reserve issued the *Interagency Guidelines Establishing Information Security Standards*.

Technology created by the Federal Financial Institutions Examination Council (FFIEC).[8] The primary purpose of the rating system is to assess risks introduced by information technology at institutions and service providers, and to identify those institutions requiring supervisory attention.[9] When examinations identify risks and weak management practices at institutions, regulators may use enforcement procedures to address such risks.[10]

The FDIC uses the Information Technology Risk Examinations (InTREx) work program to conduct IT examinations at financial institutions. The FDIC introduced InTREx in 2016 to enhance IT supervision by providing examiners with more efficient and risk-focused examination procedures.[11] From January 2016 through October 2018, FDIC examiners conducted more than 3,000 InTREx examinations by reviewing bank documentation, interviewing key personnel, testing controls, and observing. According to the Division of Risk Management Supervision (RMS) officials, FDIC personnel and other regulators are considering InTREx enhancements to increase the effectiveness of the work program. One example would be using data to review and understand cybersecurity risks across all institutions.

InTREx examinations required more hours than the prior examination methodology and impacted the FDIC's ongoing challenge to ensure that it has an appropriate number of IT examiners. For example, the New York Regional Office stated that the InTREx examination process increased an average of 67 percent over the prior IT examinations, thus adding an extra 80 hours to the examination. In its operating budget for 2019, the FDIC added 23 positions to its IT examination workforce in recognition of growing cybersecurity risks, including those posed by TSPs.

Another challenge is keeping examiner skills current and up-to-date. The FDIC aims to match examiner skills with the complexity and sophistication of IT environments at banks. Changes in technology can affect the risk profile of an individual bank. For example, in the planning phase of an IT examination, the FDIC may find that the risk profile of a bank has increased and is greater than previous FDIC projections. Therefore, the FDIC may be required to shift examination staffing resources on short notice. We have work underway to review IT examination staffing and the effectiveness of IT examinations.

Third-Party Service Providers

In addition, banks frequently hire third-party Technology Service Providers (TSP) to perform operational functions on behalf of the bank—such as IT operations and business product lines.

---

[8] The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The Council is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the OCC, and the Bureau of Consumer Financial Protection and to make recommendations to promote uniformity in the supervision of financial institutions.

[9] FFIEC, *Uniform Rating System for Information Technology*, 64 Fed. Reg. 3109 (January 20, 1999).

[10] FDIC, *Risk Management Manual of Examination Policies*, Part I 1.1 Basic Examination Concepts and Guidelines and Part IV Administrative Enforcement Actions.

[11] Financial Institution Letter-43-2016, *Information Technology Risk Examination (InTREx) Program* (June 30, 2016).

TSPs may further sub-contract services to other vendors. According to the OCC, banks are increasingly reliant upon TSPs and sub-contractors, and such dependence creates a high level of risk for the banking industry.[12] The OCC indicates that TSPs are increasingly targets for cybercrimes and espionage and may provide avenues for bad actors to exploit a bank's systems and operations. For example, on December 20, 2018, two Chinese nationals were charged with computer intrusion offenses related to more than 45 service providers whose clients included the banking and finance industry and the U.S. Government. The hackers targeted service providers in order to gain unauthorized access to the computer networks of their clients and steal intellectual property and confidential business information.[13]

A financial institution must manage the interconnections, system interfaces, and systems access of TSPs and sub-contractors and must implement appropriate controls.[14] Significant consolidation among TSPs caused large numbers of banks—especially community banks supervised by the FDIC—to rely on a few large service providers for core systems and operations support.[15] As a result, a cybersecurity incident at one TSP has the potential to affect multiple financial institutions.[16]

FDIC examiners assess financial institutions' management of TSP risk through InTREx IT examinations.[17] The *Interagency Guidelines Establishing Information Security Standards* require that financial institutions:

- Exercise appropriate due diligence in selecting TSPs;
- Require TSPs to implement appropriate measures to meet the Interagency Guidelines objectives related to protecting against unauthorized access to, or use of, sensitive customer information; and
- Monitor contract compliance by the TSPs, including service provider audits, test results summaries, or other evaluations.[18]

A financial institution's Board of Directors and senior managers are responsible for the oversight of activities conducted by a TSP on their behalf to the same extent as if the activity were handled within the institution.[19]

---

[12] The FFIEC described the term TSP to include "independent third parties, joint venture/limited liability corporations, and bank and credit union service corporations that provide processing services to financial institutions." Supervision of Technology Service Providers, FFIEC IT Examination Handbook InfoBase.

[13] Department of Justice Press Release, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information* (December 20, 2018).

[14] OCC *Semiannual Risk Perspective* (Spring 2018), 18.

[15] OCC *Semiannual Risk Perspective* (Spring 2018), 18.

[16] OCC *Semiannual Risk Perspective* (Spring 2018), 18.

[17] TSPs are also subject to interagency examination by Federal regulators, including the FDIC. See Federal Regulatory Agencies' Administrative Guidelines, Implementation of Interagency Programs for the Supervision of Technology Service Providers (October 2012).

[18] These Interagency Guidelines can be found in the FDIC Rules and Regulations, Part 364, Appendix B.

[19] Financial Institution Letter 44-2008, *Guidance for Managing Third-Party Risk* (June 6, 2008).

In our prior OIG report entitled *Technology Service Provider Contracts with FDIC-Supervised Institutions* (2017), we did not see evidence, in the form of risk assessments or contract due diligence, that sampled financial institutions fully considered and assessed the potential impact and risk of TSPs. We made two recommendations to the FDIC. Although both remain unimplemented at the time of completion of this Top Challenges report, the FDIC has been working to address the recommendations.[20] We plan to conduct additional work in this area to assess whether FDIC programs ensure that institutions are properly managing risks associated with third-party relationships.

The FDIC plays an important role in addressing financial institutions' cybersecurity risk which, if left unchecked, could threaten the safety and soundness of institutions as well as the stability of the financial system. The FDIC must ensure that IT examinations assess how financial institutions manage cybersecurity risks, including risks associated with TSPs, and address such risks through effective supervisory strategies.

2 | ADAPTING TO FINANCIAL TECHNOLOGY INNOVATION

FDIC policymakers and examiners must keep pace with the adoption of new financial technology to assess its impact on the safety and soundness of institutions and the stability of the banking system. The pace of change and breadth of innovation requires that the FDIC create agile and nimble regulatory processes, so that it can respond to, and adjust policies, examination processes, supervisory strategies, preparedness and readiness, and resolution approaches, as needed.

The Group of Twenty's Financial Stability Board (FSB) defined financial technology as "innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services."[21] Financial technology innovation includes, for example, mobile wallets, digital currencies, and digital financial advice.[22] The rapid pace of financial technology is being driven

[20] The FDIC's OIG's Report on Unimplemented Recommendations contains information about recommendations from our audits and evaluations that the OIG has not closed because our Office has not determined that the FDIC has fully implemented recommended corrective actions. The status of each recommendation is subject to change due to the FDIC's ongoing efforts to implement them, and the OIG's independent review of information about those efforts. The Unimplemented Recommendations listing is updated monthly.

[21] *Financial Stability Implications from FinTech, Supervisory and Regulatory Issues That Merit Authorities' Attention*, (June 27, 2017), 7. The FSB was chartered by the Group of Twenty (G20) on September 25, 2009. The G20 Members include Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States, and the European Union (plus Hong Kong, Singapore, Spain and Switzerland). The FSB charter aims to promote global financial stability by coordinating the development of regulatory, supervisory, and other financial sector policies and conducts outreach to non-member countries. The G20 members represent about two-thirds of the world's population, 85 percent of global gross domestic product, and over 75 percent of global trade.

[22] Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018).

by capital investment, demand for speed and convenience, and digitization.[23] According to the Department of the Treasury (Treasury Department), from 2010 to 2017, more than 3,330 new technology companies were formed to serve the financial industry.[24] The Treasury Department also estimated that one-third of online U.S. consumers use at least two financial technology services—including financial planning, savings and investment, online borrowing, or some form of money transfer and payment.[25] Further, KPMG estimated that global investment in financial technology was $57.9 billion in just the first 6 months of 2018.[26]

Regulators Need Nimble Approach to Financial Innovation

The Treasury Department encouraged "an agile approach to regulation that can evolve with innovation" and stated that regulators, including the FDIC, must be nimble to adapt regulatory approaches to banks' adoption and use of emerging technology, without creating barriers to innovation.[27] According to the Basel Committee on Banking Supervision, financial technology innovation poses three main risks to the banking sector and consumers.[28]

> **Cybersecurity Risk –** Financial technology companies are interconnected with IT systems at banks, yet these technology companies may not be subjected to regulatory requirements for safety and soundness and may not be examined by financial regulators. Certain banks reported that between 20 and 40 percent of online banking logins are attributable to financial technology companies, and many banks represented that they cannot distinguish among computer logins, as to whether they originate from consumers, data aggregators, or even malicious actors.[29] IT system interconnections may provide a pathway for a cybersecurity incident at a financial technology company to infect the banking system.
>
> **Operational Risk –** When institutions have multiple technology services and relationships, they face ambiguity and uncertainty as to the applicability of certain privacy rules, the Bank Secrecy Act (BSA) provisions and regulations, and Anti-Money Laundering (AML) standards. Banks may be unsure as to whether they or the service provider implement rules, regulations, and requirements. Moreover, financial institutions face challenges to have sufficient skilled staff and capabilities to monitor these risks and

---

[23] Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* July 2018); Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Bank and Bank Supervisors* (February 2018).
[24] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018).
[25] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (July 2018).
[26] KPMG, *The Pulse of Fintech 2018: Biannual Global Analysis of Investment in Fintech* (July 2018). KPMG is a professional services company.
[27] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, 9 and 13; and *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018), 24.
[28] Basel Committee on Banking, *Sound Practices – Implications of Fintech Developments for Banks and Bank Supervisors* (February 2018).
[29] Lael Brainard, Member, Board of Governors of the Federal Reserve System, *Where Do Banks Fit in the Fintech Stack?* Remarks delivered at the Northwestern Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research & Practice" (April 29, 2017).

operations of financial technology companies. In addition, banks may find it difficult to authenticate customers under the BSA/AML requirements ("know your customer"), due to increased automation and distribution of services and products. Such opacity may lead to inadequate and deficient compliance with legal standards and requirements.

Strategic Risk – Traditional banks risk losing substantial market share and profits due to financial innovation. For example, large-scale use of distributed ledger technology[30] to process payments, such as the use of blockchain and Bitcoin, has the potential to disrupt the banking sector's payment system.

The FDIC should ensure that banks have proper governance and risk management practices around these technologies. The FDIC may need to increase training and adjust staffing to ensure examiners have the skills to effectively supervise the risks involved with new technology. Further, the FDIC may need to modify examination policies and procedures that pre-date financial innovation to improve supervision of financial innovation risk. The FDIC also must monitor for potential disruption to the banking sector from technological change and anticipate losses to the Deposit Insurance Fund.

The FDIC Chairman noted in October 2018 that "[w]hat is different today is the speed and tremendous impact of technological innovation *in* and *on* banking, and the potential for technology to disrupt not just an institution or two, but banking as we know it." As such, the FDIC Chairman announced that the agency was planning to set up an Office of Innovation, which would review how the FDIC can promote technological development at community banks, while still providing a safe regulatory environment.[31] We will continue to monitor the developments and activities of this new Office at the FDIC.

Financial technology innovation continues to grow and impact the banking system. Institutions must have robust and effective governance and management practices to mitigate risks associated with adoption of financial technology. The FDIC should evaluate the impact of these innovations on banks, assess emerging risks, and expeditiously adjust its processes and supervisory strategies.

[30] According to the National Institute of Standards and Technology (NIST), distributed ledgers, such as blockchains, are tamper-resistant digital records of transactions that once established cannot be changed. Blockchain Technology Overview, NIST Internal Report 8202.

[31] FDIC Chairman McWilliams noted her plans for an Office of Innovation in remarks at the Federal Reserve Bank of Philadelphia, "Fintech and the New Financial Landscape" (November 13, 2018).

3 | STRENGTHENING FDIC INFORMATION SECURITY MANAGEMENT

The FDIC maintains thousands of terabytes of sensitive data within its IT systems and has more than 180 IT systems that collect, store, or process Personally Identifiable Information (PII) of FDIC employees; bank officials at FDIC-supervised institutions; and bank customers, depositors, and bank officials associated with failed banks. FDIC systems also hold sensitive supervisory data about the financial health of banks, bank resolution strategies, and resolution activities. The FDIC must continue to strengthen its implementation of governance and security controls around its IT systems to ensure that information is safeguarded properly.

The U.S. Computer Emergency Readiness Team (US-CERT) reported 35,277 information security incidents for Federal Executive Branch civilian agencies in 2017. In May 2018, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) conducted a review of Federal cybersecurity capabilities at 96 civilian agencies across 76 metrics to determine each agency's ability to identify, detect, respond, and recover from cyber incidents. The review found that 74 percent (71 agencies) had cybersecurity programs that were either "At Risk" or "High Risk.[32]

As a bank regulator, the FDIC collects and maintains a significant volume of sensitive PII, such as names, home addresses, Social Security Numbers, dates and places of birth, bank account numbers, and credit card information.[33] The FDIC also maintains business proprietary information that is sensitive, including banks' internal operations regarding counterparties, vendors, suppliers, and contractors.

The FDIC has encountered a number of information security incidents over the last several years. In August 2011, the FDIC began to experience a sophisticated, targeted attack on its own network whereby an entity gained unauthorized access to the network, escalated its privileges, and maintained an ongoing presence in the network. The attacker penetrated more than 90 workstations or servers within the FDIC's network over a significant period of time, including computers used by a former Chairman and other senior FDIC officials, and gained unauthorized access to a significant quantity of sensitive data.

During late 2015 and early 2016, the FDIC experienced eight additional incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven incidents involved PII, including Social Security Numbers, and thus constituted data breaches. In the eighth incident, the departing employee took highly sensitive components of resolution

[32] *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018). "At Risk" meant that some essential policies, processes, and tools were in place to mitigate overall cybersecurity risk, but significant gaps remained; and "High Risk" meant that fundamental cybersecurity policies, processes, and tools were either not in place or not deployed sufficiently.

[33] PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

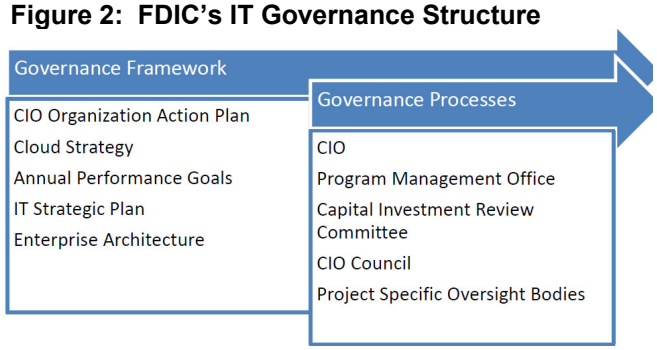
plans submitted by certain large systemically important financial institutions without authorization; this former FDIC employee was recently convicted for theft of government property.[34] Our OIG Special Inquiry[35] regarding these breaches revealed systemic weaknesses that hindered the FDIC's ability to respond to multiple information security incidents and breaches efficiently and effectively. We made 13 recommendations in our OIG Special Inquiry report; of these recommendations, 5 remained unimplemented at the time of completion of this Top Challenges report.

IT Governance

The FDIC relies extensively on IT to accomplish its mission and must subject its IT initiatives to appropriate governance and oversight. IT governance provides organizations with a structured process to support IT investment decisions while promoting accountability, due diligence, and the efficient and economic delivery of IT services.[36] As illustrated in Figure 2, the FDIC's IT governance structure consists of two principal elements:

- **The Governance Framework.** Reflects the goals and priorities of the FDIC through multiple components, including the IT Strategic Plan and Enterprise Architecture.
- **The Governance Processes**. Consist of controls and procedures to make IT capital investments and oversee individual projects.

Figure 2: FDIC's IT Governance Structure



Source: OIG analysis of IT governance documentation.

In our OIG report entitled *The FDIC's Governance of Information Technology Initiatives* (July 2018), we found that the FDIC faced a number of challenges and risks related to the governance of its IT initiatives. For example, the FDIC did not fully develop a strategy to move IT services and applications to the cloud or obtain the acceptance of key FDIC stakeholders before taking steps to initiate cloud migration projects. The FDIC also had not implemented an effective Enterprise Architecture to guide the three IT initiatives we reviewed or the FDIC's broader transition of IT services to the cloud. An ineffective Enterprise Architecture limited the FDIC's ability to communicate to business stakeholders how it intended to implement its new IT strategies. In turn, this caused stakeholders to question the decision to adopt new cloud technologies and the impact on business processes. We made eight recommendations to

[34] United States Attorney's Office, Eastern District of New York, Department of Justice Press Release, *Former Senior Employee at FDIC Convicted of Embezzling Confidential Documents* (December 11, 2018).
[35] *OIG Special Inquiry Report, The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (April 2018).
[36] OIG Report, *The FDIC's Governance of Information Technology Initiatives* (July 2018).

improve the FDIC's governance processes, two of which remained unimplemented at the time of completion of this Top Challenges report.

Information Security Controls

In our annual Federal Information Security Modernization Act (FISMA) audit report, *The FDIC's Information Security Program – 2018* (October 2018), we identified security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. Although the FDIC was working to address previously identified control weaknesses, the FDIC had not yet completed corrective actions for eight prior recommendations (as of December 2018). We made four additional recommendations in this report. The following briefly describes the highest risk areas and weaknesses that can be described in a public report:

- **Information Security Risk Management.** The FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems. Notably, the FDIC had not finalized a Risk Appetite, Risk Tolerance Level, and Risk Profile. Without these fundamental elements, the FDIC faced difficulties integrating risk into its budget, strategic planning, performance reporting, and internal controls.

- **Enterprise Security Architecture.** The FISMA audit report issued in 2017 recommended that the FDIC develop an enterprise security architecture and integrate it into an enterprise architecture consistent with the Federal Government's enterprise architecture requirements and the FDIC's business and mission requirements. According to NIST, an enterprise security architecture describes the structure and processes of an organization's security processes, information security systems, and responsibilities of personnel and units, and shows their alignment with the organization's mission and strategic plans. The lack of an effective enterprise security architecture increases the risk that the FDIC's information systems could be developed with inconsistent security controls that are costly to maintain. In July 2018, the FDIC provided the OIG with documentation describing its enterprise security architecture. The OIG is reviewing the corrective actions undertaken by the FDIC at the time of this Top Challenges report.

- **Security Control Assessments.** FISMA requires agencies to test and evaluate their information security controls periodically to ensure they are effectively implemented. We identified instances in which security control assessments performed by contractors did not include testing of security control implementation. Instead, assessors relied on narrative descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without actual testing, assessors did not have a basis for concluding on the effectiveness of security controls. Moreover, we found that the FDIC did not

have adequate oversight of security control assessments performed by contractor personnel.

- **Patch Management.** Software vendors release patches as needed or on a periodic basis to address faults in operating systems or applications. Vendors may also issue patches to alter functionality, address new security threats, or modify software configurations to improve security. Effective patch management is, therefore, critical to maintaining the integrity, availability, and security of the FDIC's IT infrastructure and the data that resides within it. We found that the FDIC's patch management processes were not always effective in ensuring that the FDIC implemented patches within defined timeframes. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.

- **Backup and Recovery.** Our FISMA audit report issued in 2017 noted that the FDIC's IT restoration capabilities were limited, and that the FDIC had not taken timely action to address limitations in its ability to maintain or restore critical IT systems and applications during a disaster. The FDIC will continue to have limited assurance that it can maintain and restore mission-essential functions within applicable timeframes during an emergency, until the completion of the Backup Data Center Migration Project in 2019.

The FDIC has increased the 2019 Operating Budget for the Office of the Chief Information Security Officer by approximately $650,000 (1.3 percent), up to a total of $51 million. The increased funding is intended to enhance the protection of the FDIC's applications systems and databases from breaches and intrusions, and improve the FDIC's responsiveness and resilience.

In another OIG report entitled *Controls over System Interconnections with Outside Organizations*, (December 2018), we reviewed the FDIC's controls for managing system interconnections[37] with Federal agencies and non-governmental entities. We found that the FDIC's policies and procedures did not define the types of technologies and configurations that constituted a system interconnection and, therefore, required a written agreement. In addition, the FDIC's policies and procedures did not articulate the roles and responsibilities for all stakeholders involved in managing system interconnections. Also, the FDIC did not establish documentation requirements for key activities, and it did not create written agreements to govern several of its system interconnections. Further, we identified instances in which written agreements governing system interconnections had expired, even though the underlying connections remained enabled. We made seven recommendations to improve the FDIC's policies, procedures, and contracts governing system interconnections.

[37] NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, defines a "system interconnection" as a direct connection of two or more information technology systems for the purpose of sharing data and other information resources.

We have a number of planned and ongoing audits of the FDIC's internal IT operations, including the FDIC's privacy program and practices; security of a system that supports the FDIC's bank supervision and consumer compliance; and security of mobile devices.

The FDIC must safeguard information held within its IT systems, much of which contains sensitive information about banks, depositors, and FDIC employees. Unauthorized access and disclosure of this information could cause significant harm to individuals, banks, and the FDIC. The FDIC must remain vigilant in its efforts to institute necessary controls and properly protect the information entrusted to it.

4 | PREPARING FOR CRISES

Central to the FDIC's mission is readiness to address crises in the banking system. The FDIC must be prepared for a broad range of crises that could impact the banking sector. These readiness activities should help to ensure the safety and soundness of institutions, as well as the stability and integrity of our nation's banking system.

Crisis readiness requires advanced preparation, regardless of whether the crisis results from financial disruption in the markets, economic turmoil, a cyber attack, natural disaster, or other event. "When the unexpected, enterprise-threatening crisis strikes, it is too late to begin the planning process. Events will quickly spin out of control, further adding to the loss of reputation and avoidable costs necessary to survive and recover with minimal damage."[38]

Although crises may be different in their cause or complexity, implementation of fundamental principles allows agencies, such as the FDIC, to plan and prepare for such events. Figure 3 illustrates the Crisis Management Preparedness Cycle, which includes the following five components:[39]

Figure 3: Crisis Management Preparedness Continuous Cycle

Source: Federal Emergency Management Agency.

[38] Hastings Business Law Journal, *The Board's Responsibility for Crisis Governance* (Spring 2017), 290.
[39] Federal Emergency Management Agency National Incident Management System.

- **Plan –** Supports effective operations by identifying objectives, describing organizational structures, assigning tasks to achieve objectives, identifying responsibilities to accomplish tasks, and contributing to the goals.
- **Organize –** Identifies necessary skillsets and technical capabilities.
- **Train –** Provides personnel with the knowledge, skills, and abilities to respond to a crisis.
- **Exercise –** Identifies strengths and weaknesses through an assessment of gaps and shortfalls with plans, policies, and procedures to respond to a crisis.
- **Evaluate and Improve –** Compiles lessons learned, develops improvement plans, and tracks corrective actions to address gaps and deficiencies identified.

Early Risk Identification and Mitigation

The Financial Crisis Inquiry Commission stated that financial regulators "had ample power in many arenas [to protect the financial system], and they chose not to use it," thus rejecting the regulators' claim that they did not have the necessary authorities.[40] The current FDIC Director (former FDIC Chairman) noted that when banks are profitable, as in 2018, the FDIC and other regulators must maintain supervisory vigilance.[41]

In 2011, the FDIC developed a Forward-Looking Supervision initiative as part of the lessons learned from the financial crisis. The goal of the initiative was to "identify and assess the potential impact of an institution's new and/or growing risks and ensure early mitigation if necessary."[42] In our OIG evaluation report, *Forward-Looking Supervision* (August 2018), we found that the FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision and should clarify guidance associated with its purpose, goals, roles, and responsibilities. We also found that examiners identified overall concentration risk management conclusions and concerns in the examination report; however, only 27 percent of reports sampled elevated concerns to the financial institution's board of directors.

In addition, the FDIC uses other systems and risk-monitoring tools to identify financial institution emerging risks. For example, the Offsite Review Program (ORP) analyzes quarterly financial institution data against benchmark indicators developed by the FDIC. When an institution falls outside these benchmarks, FDIC examiners must review the bank's information, document the risks, and select an appropriate supervisory strategy to address the risks. We are currently conducting a review to examine the extent to which the ORP identifies supervisory concerns and potential problems, and appropriately adjusts supervisory strategies.

---

[40] Financial Crisis Inquiry Commission, *Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States* (January 21, 2011). The Financial Crisis Inquiry Commission was established as part of the Fraud Enforcement and Recovery Act (Public Law 111-21) to examine the causes of the financial crisis.
[41] "Financial Regulation: A Post-Crisis Perspective", Remarks by Martin J. Gruenberg, then-Chairman of the FDIC, Brookings Institution (November 14, 2017).
[42] FDIC RMS Perspectives, Vol 1, Issue 2, (Second Quarter 2014).

Crisis Preparedness and Planning

According to the FDIC's analysis of the 2008-2011 financial crisis, the events unfolded more quickly than the FDIC expected and were more severe than the FDIC's planning efforts anticipated.[43] For example, in July 2008, the FDIC resolved IndyMac, the most expensive FDIC failure, estimated to cost about $12.3 billion, and in September 2008, Washington Mutual, the sixth-largest FDIC-insured institution, also failed. The FDIC had not planned for several large and small banks to fail at the same time, and these failures occurred at a quicker pace than in previous crises.

Consequently, the FDIC needed to hire staff quickly to manage the escalating workload associated with what would ultimately be nearly 500 failed banks. To address its staffing shortfall, the FDIC authorized funding for additional personnel during the crisis but faced challenges expediting the hiring process to on-board needed staff. For example, in September 2008, the Division of Resolutions and Receiverships had an authorized staff of 825, but only 259 staff was on board.[44]

The FDIC also faced challenges dealing with the increased volume of contracts needed. During the financial crisis, the FDIC awarded over 6,000 contracts totaling more than $8 billion. The size of its acquisition staff was initially insufficient, which resulted in delays to modify existing contracts and issue new contracts. The FDIC needed to rapidly hire and train personnel to oversee the contracts.

Over the past several years, the FDIC developed goals and objectives to prioritize certain crisis readiness planning activities. According to the FDIC 2018-2022 Strategic Plan, the agency aims to "develop, test, and maintain contingency plans to ensure it is prepared to handle a wide range of potential failure scenarios, including the failure of a large financial institution; simultaneous, multiple failures; the failure of an institution with large international holdings; and the failure of an insured institution that operates primarily through the internet." The FDIC is developed a draft "surge staffing" plan that addresses resources needs for concurrent community bank failures in conjunction with the failure of a moderately large ($25 to $50 billion) bank.

We are conducting an evaluation to assess the FDIC's preparedness efforts to address future crises. The scope of our evaluation includes examining the FDIC's crisis readiness plans, its tools and mechanisms to implement the plans, roles and responsibilities, training on crisis response, and actions to evaluate and improve readiness.

The FDIC's ability to mitigate risk and resolve failed banks affects the safety and soundness of institutions as well as the stability of the banking system. The FDIC should maintain robust processes to plan, prepare, train, exercise, and maintain readiness for scenarios that could lead to crises.

---

[43] FDIC, *Crisis and Response, An FDIC History, 2008-2013* (November 30, 2017).
[44] *Crisis and Response, An FDIC History, 2008-2013.*

5 | MATURING ENTERPRISE RISK MANAGEMENT

Enterprise Risk Management (ERM) is a critical part of an agency's governance, as it can inform prudent decision-making at an agency, including strategic planning, budget formulation, and capital investment. ERM program requirements include identifying risks that could affect the organization (Risk Profile and Inventory), establishing the amount of risk an organization is willing to accept (Risk Appetite), prioritizing strategies to address risks in the proper sequence, and responding to and mitigating the risks. The FDIC established an ERM program office in 2011, but has neither developed the underlying ERM program requirements nor realized the benefits of a mature ERM program.

According to FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program*, "Congress, the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) have directed attention to the need for federal agencies to adopt [Enterprise Risk Management (ERM)]." OMB introduced ERM through revised government-wide circulars, including OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. The FDIC Directive states that while not legally obligated to follow executive directives, the FDIC "embrace[s] the spirit of ERM as outlined in OMB Circular No. A-123."[45]

According to OMB Circular No. A-123, Federal agencies face internal and external risks to achieving their missions, including "economic, operational, and organizational change factors, all of which would negatively impact an Agency's ability to meet goals and objectives if not resolved."[46] OMB Circular No. A-123 further requires that agencies take risk into account when designing internal controls. ERM should be an element of the agency's overall governance process that focuses specifically on the identification, assessment, and management of risk, and it should include these elements:

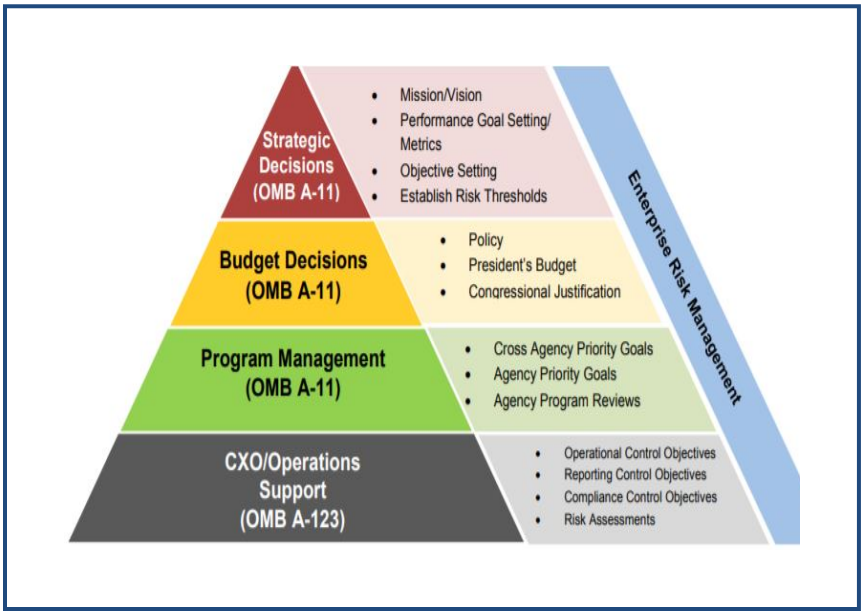
- A risk management governance structure;
- A methodology for developing a risk profile; and
- A process, guided by an organization's senior leadership, to consider risk appetite and risk tolerance levels that serves as a guide to establish strategy and select objectives.

OMB urges agencies to adopt an enterprise-wide view of ERM—a "big picture" perspective—thus synthesizing the management of risks into the very fabric of the organization; it should not be viewed in "silos" among different divisions or offices. ERM should integrate risk management into the agency's processes for budgeting, including strategic planning, performance planning, and performance reporting practices.

[45] OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, (July 15, 2016).
[46] OMB Circular No. A-123 (July 5, 2016), 7.

Figure 4: Enterprise Risk Management Program

Figure 4 illustrates the manner in which ERM should be implemented in an organization, and the junctures at which it should be considered when making decisions concerning the agency's strategy, budget, program management, and operations. Effective ERM implementation starts with an agency establishing a customized ERM program that fits its organizational mission, culture, operating environment, and business processes.



Source: Playbook: Enterprise Risk Management for the U.S. Federal Government.

GAO identified six essential elements to assist Federal agencies' implementation of ERM, including:[47]

1. **Align the ERM process to agency goals and objectives** – Ensuring that ERM contributes to achieving mission and results.
2. **Identify Risks** – Assembling a list of risks and opportunities that could affect the agency from achieving its goals and objectives.
3. **Assess Risks** – Prioritizing risk responses based on an assessment of the likelihood and impact of a risk on the agency's mission.
4. **Select Risk Response** – Selecting a strategy to respond to or mitigate risk based on management's risk appetite, such as acceptance, avoidance, reduction sharing, or transfer of risk.
5. **Monitor Risks** – Determining whether risks are changing and if responses are successful.
6. **Report on Risks** – Communicating with management and other stakeholders on the status of addressing risks.

The FDIC's Enterprise Risk Management Program

In June 2010, the FDIC hired a consulting firm to address five key issues regarding its ERM program: Identification and management of risks; Organizational structure; Risk management activities and processes; Capabilities and infrastructure for risk management; and Actionable transparency. The consulting report identified gaps in all five areas, recommended that the FDIC establish a Chief Risk Officer (CRO), and submitted several organizational options to be evaluated by the FDIC. In response to the firm's recommendations, the then-FDIC Chairman

[47] GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, GAO-17-63 (December 1, 2016).

appointed a Risk Steering Committee to evaluate alternatives and recommend an organizational structure for risk management.

The Risk Steering Committee recommended to the FDIC Board the establishment of an Office of Corporate Risk Management (OCRM), headed by a CRO, with total staffing of 16. The Board approved changes recommended by the Risk Steering Committee in January 2011. The changes were intended to provide an office within the FDIC that was assigned to review internal risks with a system-wide perspective; facilitate sharing of information regarding existing, emerging, and potential risks; and instill risk governance as part of the FDIC's culture.

By May 2016, the CRO had retired and only five staff remained in OCRM by 2017. Consequently, in 2017, the FDIC initiated an organizational review of its existing ERM program to assess whether changes to the program should be made based on its experience-to-date with its ERM framework. In June 2017, the FDIC placed the CRO under the Division of Finance (DOF) as a Deputy Director, and combined OCRM with the Corporate Management Control Branch, to form a newly constituted Risk Management and Internal Controls Branch (RMIC) within DOF. RMIC responsibilities included not only ERM, but also internal control as well as management of risks in individual programs and projects.

The FDIC, in its 2018 Performance Goals, identified enterprise risk as a priority initiative.[48] However, as noted above, we reported in our recent FISMA audit, *The FDIC's Information Security Program – 2018* (October 2018) that the FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks. The FDIC had not finalized its Risk Appetite, Risk Tolerance Level, and Risk Profile. Without these key fundamental elements, the FDIC faced difficulties integrating risk into its budget, strategic planning, performance reporting, and internal controls. In addition, FDIC Divisions and Offices were not able to evaluate risk determinations in the context of the agency's overall risk levels, tolerance, and profile. As a result, the FDIC could not be sure that its resources were being allocated toward addressing the most significant risks in achieving strategic objectives.

The FDIC issued its revised *Enterprise Risk Management and Internal Control Program Policy* (ERM Policy) in October 2018.[49] This ERM Policy aims to "identify, assess, and address major risks (including emerging risks) that have a potential broad impact to the FDIC's ability to achieve its goals, objectives, and mission." The ERM Policy indicates that the agency's ERM would be implemented through the FDIC's existing structure, and that FDIC Divisions and Offices would identify key activities and risks, and take actions to address these risks.

The FDIC's ERM Policy identified key requirements for the program, including establishing a Risk Appetite and Risk Profile. The ERM Policy also requires that the FDIC establish a Risk Inventory which is a "comprehensive, detailed list of risks that could affect the FDIC's ability to

[48] 2018 FDIC Performance Goals, Priority 2018 Initiatives, Goal 6: Identify and address enterprise risk.
[49] FDIC, *Enterprise Risk Management and Internal Control Program*, Directive 4010.3 (October 25, 2018).

meet its strategic objectives," and that the ERM program includes the following essential elements:

- Process Alignment to Goals and Objectives;
- Risk Identification;
- Risk Assessment;
- Risk Response Selection;
- Risk Monitoring; and
- Communication and Reporting.

We are initiating an evaluation of the FDIC's ERM program to assess the extent to which the FDIC has implemented an effective ERM program consistent with guidance and best practices.

The FDIC should develop an integrated approach to ERM. This ERM program should synthesize the management of risks into the FDIC's organizational culture, so that these risks may be considered and incorporated into the FDIC's budget, strategic planning, performance reporting, and internal controls for the agency as a whole.

6 | SHARING THREAT INFORMATION WITH BANKS AND EXAMINERS

Federal Government agencies and private-sector entities share information about threats to U.S. critical infrastructure sectors, including the financial sector. Sharing actionable and relevant threat information among Federal and private-sector participants protects the financial system by building threat awareness and allowing for informed decision-making. The FDIC must ensure that relevant threat information is shared with its supervised institutions and examiners as needed, in a timely manner, so that actions can be taken to address the threats. Threat information also provides FDIC examiners with context to evaluate banks' processes for risk identification and mitigation strategies.

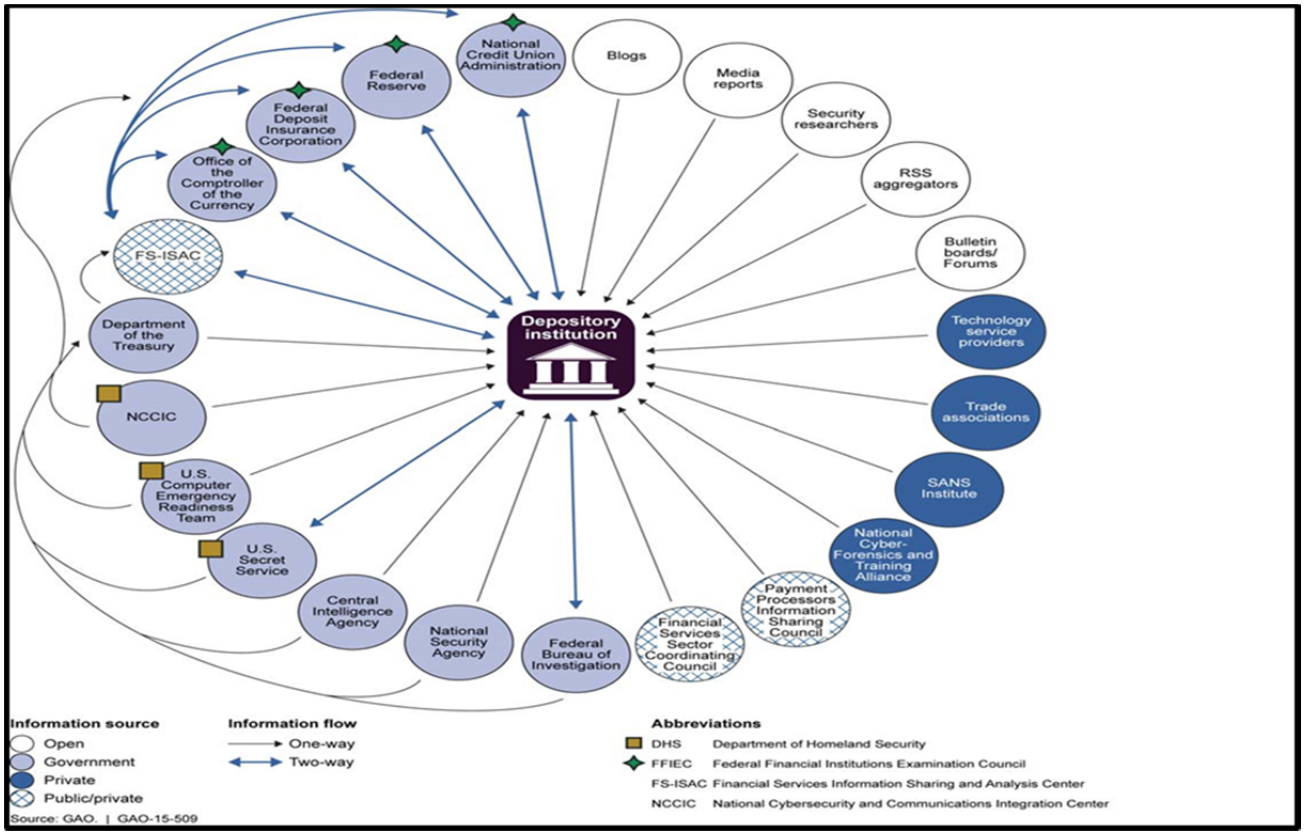
Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, identified the financial services sector as one of 16 critical infrastructure sectors vital to public confidence and the nation's safety, prosperity, and well-being. The FFIEC recognized that financial institutions should be prepared to address a variety of threats, including terrorists attacks, pandemics, and cybersecurity.[50] For example, cyberattacks at financial institutions prevented public access to websites, compromised personal information of tens of millions of customers, and millions of dollars were lost due to systems breaches where criminals transferred funds from customer accounts and from automated teller machines.[51] Further, information such as that provided by the Centers for Disease Control and Prevention allows financial institutions to monitor potential

[50] FFIEC, *Business Continuity Planning* (February 2015).
[51] GAO, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*, GAO-15-509 (July 2015).

pandemic health outbreaks to ensure institutions have the capability to continue critical operations when large numbers of staff are unavailable for prolonged periods of time.[52]

FSOC noted, in its 2018 Annual Report, the critical importance of sharing timely and actionable threat information among the Federal Government and the private sector. FSOC stated that Federal agencies should consider how to share information and when possible "declassify (or downgrade classification) of information to the extent practicable, consistent with national security needs."[53] GAO also identified various sources of threat information that could be shared with financial institutions. Figure 5 illustrates how GAO captured threat information flows from multiple sources.

Figure 5: Selected Sources of Threat Information



In July 2018, DHS launched a new initiative called the National Risk Management Center (NRMC). According to DHS, the NRMC was established in response to "the increasingly complex threat environment and corresponding demand from industry for greater integrated support from the U.S. federal government."[54] The NRMC will work across industry sectors and Federal agencies, including the banking sector, so that participants can have a more comprehensive perspective on systemic risk; the goal is to promote collaborative risk strategies.

[52] Centers for Disease Control and Prevention *Pandemic Intervals Framework*, (September 26, 2014); and FFIEC, *Business Continuity Planning*, Appendix D: Pandemic Planning.
[53] FSOC 2018 Annual Report, 7.
[54] DHS, National Risk Management Center Fact Sheet (July 2018).

According to the FDIC's 2017 Annual Report, the FDIC continues to engage with the Financial and Banking Information Infrastructure Committee, Financial Services Sector Coordinating Council for Critical Infrastructure Protection, DHS, and other regulatory agencies and law enforcement to share information and coordinate responses.

Banks' Access to and Use of Threat Information

In November 2014, the FDIC and other FFIEC members encouraged financial institutions to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), through its *Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing* (*Cybersecurity Sharing Statement*).[55] FS-ISAC is a group of 7,000 member organizations, and its purpose is to share timely, relevant, and actionable security threat information. The *Cybersecurity Sharing Statement* also suggested using other resources such as the Federal Bureau of Investigation's (FBI) InfraGard,[56] U.S. Computer Emergency Readiness Team,[57] and Secret Service Electronic Crimes Task Force.[58]

According to the FFIEC, financial institutions should have business continuity plans that "[a]nalyze threats based upon the impact to the institution, its customers, and the financial market it serves."[59] Further, the FFIEC notes that financial institutions should have "a means to collect data on potential threats that can assist management in its identification of information security risks."[60] FDIC-supervised institutions are links of the chain in the financial services system interconnections; an incident involving one community bank has the potential to affect the broader financial sector.[61] Therefore, as part of its examination process, the FDIC must ensure that supervised institutions can receive and access threat information, and that they have business continuity plans to address such threats.

FDIC and Examiners' Access to and Use of Threat Information

FDIC Headquarters staff has access to significant amounts of threat information held by the U.S. Government, and much of the information is confidential and highly sensitive. The FDIC should develop sound practices to review threat information and take necessary actions based upon such information. In doing so, the agency should ensure that it develops and maintains processes to assess the sensitivity and classification of this information.

---

[55] FFIEC, *Statement on Cybersecurity Threat and Vulnerability Monitoring and Sharing*.
[56] InfraGard is a web-based portal that provides collaboration between the FBI and the private sector to exchange information about critical infrastructure.
[57] US-CERT is a component of the Department of Homeland Security; its mission is to reduce the nation's risk of systemic cybersecurity and communications challenges.
[58] The Electronic Crimes Task Force is a nationwide network designed to support and assist state, local, and Federal law enforcement agencies in order to combat criminal activity involving the use of new technology.
[59] FFIEC, Business Continuity Planning Booklet, *Risk Assessment*, (Available on the FFIEC website).
[60] FFIEC IT Examination Handbook Infobase, Information Security Booklet, II, *Information Security Program Management* (Available on the FFIEC website).
[61] Departments of the Treasury and of Homeland Security, *Financial Services Sector-Specific Plan* (2015), 9.

In addition, the FDIC should ensure that the threat information can be disseminated to specific examiners as needed, and that such examiners are authorized to receive access to sensitive threat information. For example, if the FDIC has access to threat information about a particular FDIC-supervised bank, the examiners overseeing this institution should have access to such threat information. Given the volume of information, the FDIC faces challenges to analyze, distill, and convey relevant and actionable threat information from FDIC Headquarters to examiners in the FDIC's Regional and Field Offices.

Threat information can assist FDIC examiners in prioritizing and focusing their work on emerging issues, and modifying the depth or scope of an examination. Understanding the nature of threats provides context for examiners when evaluating financial institutions' processes for identifying and considering relevant risks and implementing risk mitigation strategies. Further, threat information may result in changes to examination policy or procedures to address emerging issues.

RMS instituted *Regional Cyber Incident Reporting and Response Guides* (Reporting and Response Guides) to outline the steps to be taken by Regional and Field Offices when banks report threats and incidents. These steps include gathering information about an incident; providing advice to the affected entity; determining whether the incident warrants escalation to FDIC Headquarters; and conducting ongoing monitoring and communications. RMS also has a *Cyber Incident Response Plan* for use by FDIC Headquarters staff to evaluate threats and incidents reported by banks through the Field and Regional Offices. The Plan uses predetermined criteria and thresholds to determine when threat and incident information should be escalated to FDIC senior management.

Neither the RMS *Cyber Incident Response Plan* nor the Reporting and Response Guides provide procedures for the FDIC to disseminate information *to* its Regional and Field Offices and examiners. RMS officials stated that they review threat information from multiple sources and regularly convey relevant information to Regional and Field Office examiners, depending upon the criticality and sensitivity of the information.

Based on our research, as of the end of 2018, the FDIC did not have a policy that (i) defined criteria for selecting relevant, actionable threat information, or (ii) outlined the process to share such threat information among Headquarters, Regional Offices, and examiner personnel. Without policies to guide those processes, information selection and dissemination is left to the discretion of individuals, which may lead to inconsistencies, uncertainty, and a lack of uniformity in sharing threat information. We have work planned to evaluate the effectiveness of the FDIC's procedures for the collection and dissemination of threat information.

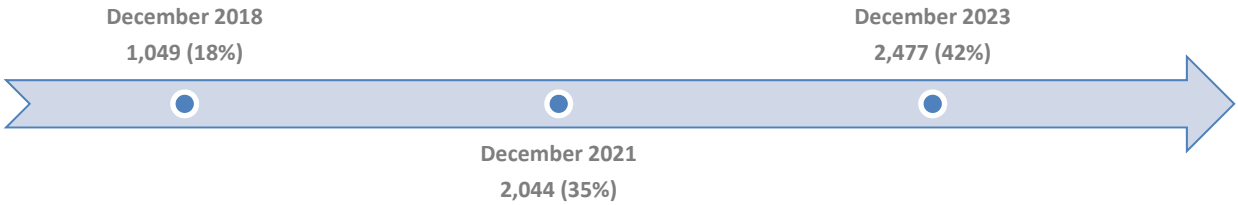
Sharing threat information allows for the consideration of these risks in developing and examining bank mitigation strategies and continuity plans. Absent such threat information, financial institutions and examiners may not have a full understanding of the risks facing the banks, and thus, risk mitigation and supervisory strategies might have gaps which could affect the safety and soundness of institutions.

7 | MANAGING HUMAN CAPITAL

The FDIC relies on skilled personnel to fulfill its mission, and about 63 percent of the FDIC's operating budget for 2019 ($2 billion) was for salaries and associated benefits for employees. Forty-two percent of FDIC employees are eligible to retire within 5 years, which may lead to knowledge and leadership gaps. To ensure mission readiness, the FDIC should find ways to manage this impending shortfall. In addition, the FDIC should seek to hire individuals with advanced technical skills needed for IT examinations and supervision of large and complex banks.

GAO has identified human capital management as a high risk since 2001 and noted that "[m]ission-critical skills gaps within the federal workforce pose a high risk to the nation."[62] GAO noted that such gaps, if left unaddressed, can "impede the federal government from cost-effectively serving the public and achieving results." The percentage of FDIC employees eligible to retire more than doubles (2.3 times) over the next 5 years, increasing from 18 percent in 2018 to 42 percent in 2023, as shown in Figure 6.

Figure 6: FDIC Employees Eligible for Retirement between December 2018 and December 2023



Source: OIG analysis of FDIC employee information as of July 31, 2018.

These figures could lead to a wave of retirements at the FDIC in the near term. As recognized by GAO, retirement waves can result in leadership voids, which could impede the capabilities of any agency to achieve its mission, unnecessarily delay decision-making, and reduce program management and oversight.[63] According to GAO, such agencies may face gaps in skillsets, which could result in the agency not being able to complete its mission-critical work in a timely manner. Further, retirements might have financial implications for the FDIC's budget, since the FDIC would be required to expend lump-sum payments based on accumulated annual leave.[64] The FDIC should be prepared to address any resultant budget issues and gaps in skillsets and leadership.

In addition, the FDIC faces an even higher rate of potential retirements among seasoned senior and mid-level managers. As of July 31, 2018, approximately two-thirds of the Executive

[62] GAO, *High-Risk Series: Progress in Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (February 2017), 61.
[63] GAO, *High-Risk Series: Progress in Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (February 2017), 61.
[64] Office of Personnel Management, Fact Sheet: Lump Sum Payment for Annual Leave.

Management employees (66 percent) were eligible to retire within 5 years, and another 57 percent of FDIC Corporate Managers are eligible in that same timeframe. Without proper succession planning strategies, these retirements can result in further leadership gaps.

Retirement Eligibility – Impact on Divisions (Headquarters and Regions)

Between 34 and 63 percent of employees in the following FDIC driver and primary support Divisions were eligible to retire within 5 years (as of July 31, 2018):

- 63 percent of employees within the Division of Resolutions and Receiverships (243 employees);
- 59 percent of employees within the Legal Division (268 employees);
- 57 percent of employees within the Division of Administration (201 employees);
- 45 percent of employees within the Division of Information Technology (133 employees);
- 38 percent of employees within the Division of Risk Management Supervision (929 employees); and
- 34 percent of employees within the Division of Depositor and Consumer Protection (276 employees).

While employees do not always retire when first eligible,[65] there is a risk that a wave of retirements could lead to gaps in leadership positions and skillsets at the FDIC. Leadership gaps can result in delayed decision-making, reduced program oversight, and failure to achieve goals and agency missions when positions are unfilled or leaders remain in acting status. Skillset gaps can undermine the ability of the FDIC to achieve its goals and missions.

In addition, in 2017, the Division of Insurance and Research (DIR) experienced higher than normal attrition rates of 13 percent. Over this period of time, 27 individuals (out of 208 in DIR) departed DIR, 74 percent of whom were specialized economists with advanced degrees. These unique skillsets may be more difficult to replace in an expanding economy.

Retirement Eligibility – Impact on Regional Offices

In the six FDIC Regional Offices, more than one-third of employees are eligible to retire within the next 5 years. Those retirements are predominantly for examination staff. Between 34 and 53 percent of employees in the FDIC Regional Offices were eligible to retire within this timeframe (as of July 31, 2018):

- 53 percent of employees within the FDIC Dallas Regional Office (413 employees);
- 38 percent of employees within the FDIC Atlanta Regional Office (176 employees);
- 37 percent of employees within the FDIC San Francisco Regional Office (164 employees);
- 34 percent of employees within the Chicago Regional Office (172 employees);

[65] Our analysis shows that employees tend to remain with the FDIC for approximately 8 years after their retirement eligibility date.

- 34 percent of employees within the Kansas City Regional Office (169 employees); and
- 34 percent of employees within the New York Regional Office (195 employees).

The FDIC is working to hire and train new examiners to address the retirement shortfall, but it takes approximately 4 years from the time an employee is hired until that employee earns an examination commission. Such commissioning requires that employees meet benchmarks, training, and other technical requirements, including passing a Technical Examination.

In its review of the financial crisis of 2008-2011, the FDIC stated that one of its strengths was "a core of seasoned examiners and supervisors."[66] These experienced employees were crucial in tailoring "informal and formal enforcement actions that helped make it possible for many banks to return to health." As noted by the FDIC in its review, the crisis experience highlighted the importance of a steady flow of new examiners who can benefit from the knowledge and experience of seasoned examiners. The FDIC may be challenged to build on innovative strategies used in prior crises for any future banking crisis without these experienced examiners and supervisors or the transfer of their knowledge to newer examiners.

Even with additional hires, Regional Offices may not have sufficient experience among their examiners. As a result, senior examiners may be required to travel more frequently in order to supervise less experienced staff and sign reports of examination (since pre-commissioned examiners cannot sign those reports). In addition, experienced examiners may be required to travel more often, in order to fill staffing needs where there have been significant retirements. This increase in travel requirements could be costly and may affect the morale of examiners, since it has been cited as the top reason for voluntary attrition by examiners.

RMS also identified a need to build out skill sets. In 2012, RMS initiated a multi-year Subject Matter Expert Project to build out workforce capacity and focus on developing advanced skills in the areas of accounting, capital markets, information technology, and anti-money laundering compliance. The FDIC also recently updated employees about a Field Office Modernization initiative, aimed, in part, to maintain a reasonable work/life balance for field examiners.

In 2013, the FDIC established a Workforce Development Initiative (WDI) to address succession planning and other workforce development challenges and opportunities. Five years after its establishment, however, the FDIC noted, in its 2018 Annual Performance Plan, that the WDI is "in the early stages of a multi-year effort to identify future workforce and leadership requirements, assess current workforce capabilities, support employees who aspire to leadership and management roles, and develop and source the talent to meet emerging workforce needs."

The management of human capital is critical to the FDIC's achieving its mission. To meet its goals and objectives, the FDIC must continue to focus on managing the life cycle of human

[66] *Crisis and Response, An FDIC History, 2008-2013* (November 30, 2017), 143-144.

capital activities – planning, recruitment, on-boarding, compensation, engagement, succession planning, and retirement programs.

8 | ADMINISTERING THE ACQUISITIONS PROCESS

The FDIC relies heavily on contractors for support of its mission, especially for IT and administrative support services. The average annual expenditure by the FDIC for contractor services over the past 5 years has been approximately $587 million. The FDIC should maintain effective controls to ensure proper oversight and management of such contracts and should conduct regular reviews of contractors. In addition, the FDIC should also perform due diligence to mitigate security risks associated with supply chains for goods and services.

According to GAO's *Framework for Assessing the Acquisition Function at Federal Agencies*, agencies should effectively manage their acquisitions process in order to ensure that contract requirements are defined clearly and all aspects of contracts are fulfilled.[67] Agencies must properly oversee contractor performance and identify any deficiencies.

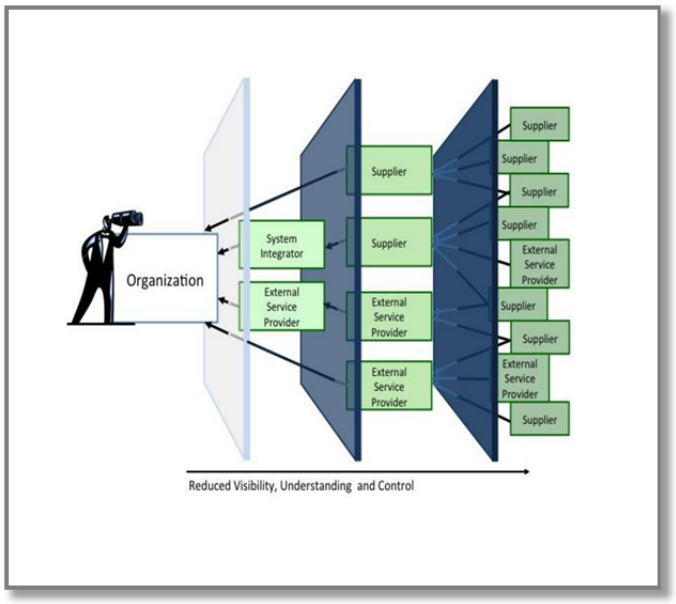
In 2018, the Administration recognized the importance of improving Federal Government acquisitions in finding that such acquisitions "often fail to achieve their goals because many Federal managers lack the program management and acquisition skills to successfully manage and integrate large and complex acquisitions into their projects."[68] In 2018, GAO reported that agencies continue to award contracts warranting increased management attention.[69] In addition, GAO found that government contracting officials were carrying heavier workloads, and thus, it was more difficult for these officials to oversee complex contracts and ensure that contractors adhered to contract terms. Further, in the *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO noted the importance of agencies defining their contracting needs and identifying, selecting, and managing providers of goods and services.

Federal Government agencies also should conduct due diligence to recognize potential threats in supply chains for products and services. When an organization hires contractors who, in turn, may sub-contract services to third-parties, the organization is likely to have reduced visibility, understanding, and control of the underlying relationships, as illustrated in Figure 7.

[67] GAO, *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO-05-218G (September 2005).
[68] The President's Management Agenda: Modernizing Government for the 21st Century, 12.
[69] GAO, *Federal Acquisitions: Congress and the Executive Branch have Taken Steps to Address Key Issues, but Challenges Endure*, GAO-18-627 (September 2018).

If not managed properly, organizations may face supply chain risks, including installation of malicious or counterfeit hardware or software, disruption of critical production, and reliance on nefarious or unqualified service providers.[70] Government agencies may not discover the consequences of these risks until much later, after the fraud or compromise

Figure 7: Supply Chain Risk View



Source: NIST Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

Contract Oversight

The FDIC awarded $2.3 billion in contracts from January 2015 through September 2018. For the first 7 months of 2018, the FDIC issued 372 contract awards for a total of $383 million. In addition, the FDIC budget for 2019 includes more than $420 million in contracting expenses for outside services.

Between January 2015 and September 2018, the Divisions of Administration (DOA), Information Technology (DIT), and Resolutions and Receiverships (DRR) accounted for 96 percent ($1.38 billion) of all contract awards through the Acquisition Services Branch. Contracting Officers are responsible for ensuring the performance of all actions necessary for efficient and effective contracting, compliance with contract terms, and protection of the FDIC's interests in all of its contractual relationships. In addition, FDIC program offices develop contract requirements, and Oversight Managers and Technical Monitors oversee the contractor's performance and technical work.

Our OIG analysis indicates that there has been an increase in the average dollar amount per contract awarded by the FDIC from 2016 to 2017. The average contract size has increased 18 percent during this time. Over the past 2 years, DRR and DIT oversaw 127 contracts valued at $1 million or more each. Many of these contracts are for computer-related and administrative services that range in value from $1 million to $98 million. According to GAO, these types of contracts require increased oversight and management attention due to the risk that contractors may perform tasks reserved for the Government.[71]

Our work has identified a number of issues related to the FDIC's contract administration. In our OIG report, *The FDIC's Failed Bank Data Services Project* (March 2017), we reviewed transition costs ($24.4 million) of a 10-year project to change information systems on failed financial institutions. We found that the FDIC faced challenges related to defining contract requirements, coordinating contracting and program office personnel, and establishing

[70] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (July 12, 2018), 7-8.
[71] GAO, *Federal Acquisitions: Congress and the Executive Branch have Taken Steps to Address Key Issues, but Challenges Endure*, GAO-18-627 (September 2018).

implementation milestones. We reported that FDIC personnel did not fully understand the requirements for transitioning failed financial institution data and services to a new contractor, or communicate these requirements to bidders in a comprehensive transition plan as part of the solicitation. Further, the FDIC did not establish clear expectations in the contract documents and did not implement a project management framework and plans.

In addition, our OIG report on the *Follow-on Audit of the FDIC's Identity, Credential, and Access Management Program* (June 2017) found that the FDIC did not maintain current, accurate, and complete contractor personnel data needed to manage Personal Identity Verification (PIV) cards, and management had not finalized and approved a plan for retiring the FDIC's legacy PIV card system.

In our OIG Memorandum, *Infrastructure Support Contract 3 (ISC-3) with CSRA, Inc.* (July 2018), we concluded that based on limited testing, while we did not see instances of inaccurate or unsupported invoices, there was an increased risk that both errors and fraudulent activity would go undetected due to the complexity of CSRA's accounting entries for contractor and subcontractor billing. Of the seven DIT individuals overseeing the contract, two individuals never took the required training on contract oversight, and the training certificates for two other individuals had already expired in 2008.

In addition, in our OIG report, *Payments to Pragmatics, Inc.* (December 2018), we determined that about 10 percent ($47,489) of the labor charges we reviewed were not adequately supported or allowable under the contract and related task orders. The unsupported labor charges were for hours billed by two subcontractor employees who did not access the FDIC's network or facilities on the days they charged the hours. In addition, we identified unallowable labor charges for work performed offsite, away from FDIC facilities.

We currently have an ongoing evaluation to assess the FDIC's contract management oversight process. The evaluation objective includes assessing the monitoring of contracts; capacity of oversight managers to oversee assigned contracts; oversight managers' experience and qualifications; and security risks posed by contractors and their personnel.

Security and Supply Chain Risk

The FDIC also must continue to ensure that its contractors and contracting personnel meet security and suitability standards for employment and access to sensitive information. In addition, contractors must meet criteria for integrity and fitness, including the elimination of conflicts of interest, adherence to ethics obligations, and security of confidential information.[72]

These protections are important since the contractors often have access to FDIC space and information and use FDIC equipment, including sensitive information related to bank closings, as well as PII for bankers, bank customers, and FDIC employees. The FDIC's DOA (Security

[72] 12 C.F.R. Part 366.

and Emergency Preparedness Section) is responsible for establishing and implementing the security policy for contractor personnel. DOA reviews include background investigations, evaluation of any derogatory information, adjudication, and approvals and clearances.[73]

In addition, NIST identified the best practices for organizations to manage security risks associated with supply chains of goods and services; these standards require the integration of risk management throughout an organization.[74] Currently, the FDIC does not have policy guidance with respect to these supply chain risks. In addition, the duty of managing supply chain risk is a collateral responsibility for the FDIC's Insider Threat Program Manager.

The FDIC also faces challenges to mitigate supply chain risk if threats are reported through highly sensitive security information. Currently, DOA acquisition staff does not have authorized access to highly sensitive security information. Therefore, if the FDIC learns of or identifies a threat to its supply chain through the receipt of such information, the FDIC would not have contracting personnel to respond to the threat, as the current staff is not authorized to access the underlying threat information.

The FDIC depends on contracts and contractors for its mission-critical systems and operations, especially in times of crisis. The FDIC should maintain strong contracting oversight and effective controls over its contractors. In addition, the FDIC should protect against supply chain and other risks posed by goods and services procured through third-party contractors and vendors.

9 | IMPROVING MEASUREMENT OF REGULATORY COSTS AND BENEFITS

Before issuing a rule, the FDIC should ensure that the benefits accrued from a regulation justify the costs imposed. The FDIC should establish a sound mechanism to measure both costs and benefits at the time of promulgation, and it should continue to evaluate the costs and benefits of a regulation on a regular basis, even after it has been issued.

In a report issued in February 2018, GAO noted that "representatives of community banks and credit unions expressed concerns about the burden that additional regulations create for them," such as increasing their overall compliance burden and adversely affecting lending.[75] In April 2018, the FDIC updated its *Statement of Policy on the Development and Review of Regulations and Policies*, and the revised policy states that once the FDIC has found the need for a regulation, "the FDIC evaluates benefits and costs, based on available information, and

[73] FDIC, Circular 1610.2, *Personnel Security Policy and Procedures for FDIC Contractors* (January 2010).
[74] NIST Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* 7.
[75] GAO, *Community Banks and Credit Unions: Regulators Could Take Additional Steps to Address Compliance Burdens,* GAO-18-213 (February 2018), 1-2.

considers reasonable and possible alternatives." While some regulations implement a statutory requirement, the FDIC should develop and maintain strong processes to measure both costs and benefits.

Analysis of Costs and Benefits

The difficulties of cost-benefit analysis lie in the uncertainty over how to measure and calculate regulatory costs.[76] For example, the FDIC experienced challenges in quantifying the costs and benefits of a proposed rule on *Recordkeeping for Timely Deposit Insurance Determination.* The FDIC engaged a contractor that initially estimated the costs of this rule at $328 million, to be incurred by 36 financial institutions (80 cents per deposit account). However, the FDIC encountered difficulties in determining the benefits of the rule, explaining that "[b]ecause there is no market in which the value of these public benefits can be determined, it is not possible to monetize these benefits." Based upon the comments received on the proposed rule, the FDIC revised the total cost in the final rule to $478 million (an increase of $150 million). The estimated cost would be allocated to covered institutions at $386 million, while the remaining costs of $92 million were to be borne by bank customers (depositors) and the FDIC.

In 2018, GAO reviewed regulatory procedures for the financial regulators and found several weaknesses with analyses done by six financial regulators, including the FDIC.[77] In particular, the regulators did not account for the burden that certain rules would have on small entities. The Regulatory Flexibility Act (RFA) requires that Federal agencies, including the financial regulators, analyze the impact of proposed regulations on small entities and consider alternatives that could lessen the regulatory burden. Alternatively, the head of the agency may certify that the rule would not pose a significant impact on a substantial number of small entities.

The then-FDIC Chairman certified that a rule would not pose a significant impact on a substantial number of small entities for over 75 percent of the rules issued by the FDIC between 2010 and 2016 that were subject to RFA requirements.[78] GAO concluded that for two of the three rules it sampled, the FDIC did not provide any supporting information for the certifications. For example, GAO found that the FDIC did not include any of the Office of Advocacy's[79] suggested components: (i) a description of the number of affected entities; (ii) the size of the economic impacts; or (iii) the justification for the certification.[80]

---

[76] Yale Law Journal, *Cost-Benefit and Other Analysis Requirements in the Rulemaking Process, Congressional Research Service* (2014); *Cost-Benefit Analysis of Financial Regulations Case Studies and Implications* (2015).
[77] GAO, *Financial Services Regulations: Procedures for Reviews under Regulatory Flexibility Act Need to Be Enhanced*, GAO-18-256 (January 2018).
[78] GAO focused only on the RFA sections and not the other regulatory analysis in the Federal Register notice, despite agencies being allowed by statute to combine analysis to avoid duplication.
[79] The Office of Advocacy is a component of the Small Business Administration and serves as a watchdog for the RFA.
[80] GAO, *Financial Services Regulations: Procedures for Reviews under Regulatory Flexibility Act Need to Be Enhanced*, GAO-18-256 (January 2018).

For the rules for which the FDIC did perform a regulatory flexibility analysis,[81] GAO reported that while the FDIC's analyses described and quantified the rules compliance costs, they did not include descriptions or assessments of regulatory alternatives, issues raised in public comments, or steps to minimize effects on small entities.[82] GAO recommended that the FDIC adopt policies and procedures to comply with RFA requirements and key aspects of Office of Advocacy and OMB guidance in order to improve consistency. The FDIC adopted additional policies and procedures in 2018; however, the GAO recommendation remains unimplemented.

In a subsequent report issued the following month, GAO found that there were additional inadequacies in the financial regulators' consideration of regulatory burden on small institutions – particularly with respect to the quantification of data and cumulative effects of regulations.[83] The Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA) requires that at least every 10 years, the FDIC must review its rules and regulations to determine if any are outdated, unnecessary, or unduly burdensome. However, GAO found that the regulators, including the FDIC, did not conduct or report on quantitative analyses as part of their EGRPRA review process. Instead, as GAO noted, "regulators generally only provided their arguments against taking actions and did not cite analysis or data to support their narrative." GAO further found that "regulators ha[d] not assessed the ways that the cumulative burden of the regulations they administer may have created overlapping or duplicative requirements." According to GAO, Congress specifically intended for EGRPRA to require regulators to measure the cumulative effect of regulations.

In August 2018, the FDIC Chairman stated that a top priority for the agency was to examine the regulatory burden on small banks. The following month, in September 2018, the FDIC issued a proposal to retire 374 of 664 Financial Institution Letters (FIL) related to risk-management supervision. These FILs contained outdated information or guidance that was available elsewhere from the FDIC. In announcing this proposal, the FDIC committed to a review of the remaining 290 FILs.[84] We are currently conducting an evaluation to determine the effectiveness of the FDIC's cost-benefit analysis process for ensuring that rules are efficient and appropriately tailored.

Financial regulations significantly affect financial institutions and bank customers, and before imposing costs on such entities, the FDIC should ensure that the benefits of the rule justify the costs associated with its implementation. To do so, the FDIC should obtain concrete, valid, and reliable data, and analyze the information, so that it can accurately measure the costs and benefits of a regulation.

---

[81] For three of the four regulatory flexibility analyses it performed, the FDIC indicated that the rules were not subject to the requirements of the RFA.
[82] GAO*, Financial Services Regulations: Procedures for Reviews under Regulatory Flexibility Act Need to Be Enhanced*, GAO-18-256 (January 2018).
[83] GAO, *Community Banks and Credit Unions: Regulators Could Take Additional Steps to Address Compliance Burdens,* GAO-18-213 (February 2018).
[84] Financial Institution Letter 46-2018, *FDIC Seeks Comment on Proposed Retirement of Certain Financial Institution Letters* (September 10, 2018).

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.