Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2020

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation
Office of Inspector General

Date: February 13, 2020

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 (OIG) 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 $7.7 trillion in deposits at about 5,250 financial institutions and directly supervises approximately 3,380 of these banks. The FDIC also oversees the resolution and receivership of failed banks, consumer financial protection, and management of the Deposit Insurance Fund.

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

- Keeping Pace with Emerging Financial Technologies;
- Enhancing the FDIC's Information Technology Security Program;
- Ensuring the FDIC's Readiness for Crises;
- Sharing Threat Information with Banks and Examiners;
- Strengthening the Governance of the FDIC;
- Overseeing Human Resources;
- Keeping FDIC Facilities, Information, and Personnel Safe and Secure;
- Administering the Acquisition Process; and
- Measuring Costs and Benefits of FDIC Regulations.

We note that these Challenges will require continued attention and vigilance by the FDIC for the foreseeable future. We anticipate that this document will be informative for policy makers, 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 the following critical areas, a number of which remain from previous years:

- Keeping Pace with Emerging Financial Technologies;
- Enhancing the FDIC's Information Technology Security Program;
- Ensuring the FDIC's Readiness for Crises;
- Sharing Threat Information with Banks and Examiners;
- Strengthening the Governance of the FDIC;
- Overseeing Human Resources;
- Keeping FDIC Facilities, Information, and Personnel Safe and Secure;
- Administering the Acquisition Process; and
- Measuring Costs and Benefits of FDIC Regulations.

We believe that the FDIC should focus its attention on these Challenges, and we hope that this document informs policy makers, 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|KEEPING PACE WITH EMERGING FINANCIAL TECHNOLOGIES

Technology is re-shaping consumers' interactions with banks, changing the way banks do business, and disrupting the banking industry. Emerging technologies promise potential benefits but also introduce risk. Increased digital interconnections with multiple avenues to access banking systems elevate cybersecurity risk because an incident at one digital juncture has the potential to infect the entire banking system. The FDIC's challenge is keeping pace with new technology and the associated risks to banks, third-party service providers, and the banking system. The key is for the FDIC to align supervisory guidance, examination procedures, and supervisory strategies with rapidly evolving risks.

Use of financial technology is having a significant impact on banks and the banking industry. Global investment in financial technologies was $37.9 billion in the first half of 2019.[1] More than half of all consumers are interacting with banks through digital means.[2] Person-to-person cashless transactions totaled more than $570 billion in 2018.[3] Consumers also prefer connectivity among financial management applications and their bank accounts.[4]

The FDIC Chairman has recognized that technology is "not simply transforming how customers access financial services; it is transforming the business of banking both in the way consumers interact with their financial institutions, and the way banks do business."[5] Banks are incorporating new technologies into bank processes and establishing partnerships with third-party financial technology companies.[6] Community banks, in particular, are working closely with technology companies to develop solutions, such as reducing the time for loan underwriting and digital credit applications.[7]

Financial technologies offer banks potential benefits but also introduce a range of risks. According to the Financial Stability Oversight Council (FSOC),[8] "[c]yber vulnerabilities in the financial system include vulnerabilities to malware attacks, ransomware attacks, denial of service attacks, data breaches, and other events. Such incidents have the potential to impact tens or even hundreds of millions of Americans and result in financial losses of billions of dollars due to disruption of operations, theft, and recovery costs."[9]

The FDIC Chairman stated that "[c]ybersecurity is the biggest threat facing America's banks."[10] The Office of the Comptroller of the Currency (OCC) similarly observed that "[o]perational risk is elevated as banks adapt to a changing and increasingly complex operating environment," and key drivers are "the need to adapt and evolve current technology systems for ongoing

[1] KPMG, *The Pulse of Fintech 2019 – Biannual Global Analysis of Investment in Fintech*, (July 31, 2019).
[2] American Banker, *10 ways technology will change banking in 2019*, (January 6, 2019).
[3] Forbes, *Venmo Versus Zelle: Who's Winning the P2P Payments War?*, (February 11, 2019).
[4] American Banker, *10 ways technology will change banking in 2019*, (January 6, 2019).
[5] Jelena McWilliams, FDIC Chairman, Remarks at the CATO Summit on Financial Regulation, *"If You Build It, They Will Come,"* (June 12, 2019).
[6] American Banker, *10 ways technology will change banking in 2019*, (January 6, 2019).
[7] Bankrate*, Community Banks Step Up Tech to Compete with Big Banks, Benefitting Customers*, (May 31, 2019).
[8] The *Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010* established FSOC, which has responsibility for identifying risks and responding to emerging threats to financial stability. FSOC brings together the expertise of Federal financial regulators (including the FDIC), an independent insurance expert, and state regulators.
[9] FSOC, 2019 Annual Report.
[10] CNN Business, *Banks could get fined for cyber breaches, top regulator says*, (August 1, 2019).

cybersecurity threats."[11] According to reports from the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), financial institutions reported 3,494 cyberattacks during the first half of 2019.[12] Small banks (less than $1 billion in assets) were the victims of nearly half (47 percent) of bank-related cybercrimes between 2012 and 2017.[13]

In the Fall of 2019, the OCC recognized elevated cybersecurity risks as "malicious actors target not only bank staff and processes but also bank customers and third parties."[14] According to *Banking Technology Vision 2019* by the consulting firm Accenture, as interconnectivity among banks, consumers, and third parties grows, "the potential points of weakness and vulnerability also multiply."[15] Hackers need only a single weakness to exploit and penetrate systems.[16]

Banks' use of advanced technology may also increase the risks of harm to consumers. For example, the OCC noted that banks' deployment of new technology may result in fair lending issues.[17] When banks use artificial intelligence, they often use algorithm models and rules that rely upon historical data.[18] If model rules are outdated or the data used in the algorithm models are not representative of the current customer population, selection bias may occur.[19]

Banks also face competitive risks from technology innovations of non-bank entities. The OCC further noted that "[b]anks face strategic risks from non-depository financial institutions, use of innovative and evolving technology, and progressive data analysis capabilities."[20] According to the *Global Payments Pulse Survey 2019* conducted by Accenture, approximately $280 billion of banks' global payment revenue is likely to be displaced by non-bank competitors in the next 6 years.[21]

Further, according to the Basel Committee on Banking Supervision, "[t]he estimated market capitalization of crypto-assets reached a historical peak exceeding $800 billion in January 2018."[22] Non-bank entities such as Facebook[23] and Walmart[24] have announced plans to introduce cryptocurrencies. These privately controlled cryptocurrencies fall outside traditional

[11] OCC, *Semiannual Risk Perspective*, (Fall 2019).
[12] New York Times, *Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc*, (July 30, 2019).
[13] Forbes, *5 Cybersecurity Myths Banks Should Stop Believing*, (April 8, 2019).
[14] OCC, *Semiannual Risk Perspective*, (Fall 2019).
[15] Accenture, *The Dawn of Banking in the Post-Digital Era – Banking Technology Vision 2019*, (May 7, 2019).
[16] New York Times, *Capital One Breach Shows How a Bank Hacker Needs Just One Gap to Wreak Havoc*, (July 30, 2019).
[17] OCC, *Semiannual Risk Perspective*, (Fall 2019).
[18] American Banker, *Don't let AI trigger a fair-lending violation*, (August 6, 2019).
[19] American Banker, *Don't let AI trigger a fair-lending violation*, (August 6, 2019).
[20] OCC, *Semiannual Risk Perspective*, (Fall 2019).
[21] Accenture, Global Payment Pulse Survey 2019.
[22] Basel Committee on Banking Supervision, *Discussion Paper: Designing a Prudential Treatment for Crypto-assets*, (December 2019).
[23] Washington Post, *Why governments around the world are afraid of Libra, Facebook's cryptocurrency*, (July 12, 2019).
[24] American Banker, *Walmart crypto coin patent could be a back door to banking*, (August 2, 2019). One bank, JP Morgan Chase, plans to issue its own cryptocurrency called JPM Coin that will be used for international payments for large institutional clients. See CNBC, *JP Morgan is tolling out the first US bank-backed cryptocurrency to transform payments business*, (February 14, 2019).

banking systems and may be beyond the reach of the current regulatory structures.[25] In addition, certain banks are also testing the use of blockchain and distributed ledger technologies, as well as digital currencies for cross-border transfers.[26]

Modernizing FDIC Guidance and Understanding Risks of Financial Technology

FDIC policy makers should understand technology and its impact on the safety and soundness of institutions in order to provide guidance to both bankers and examiners. Keeping policies and guidance in step with technology is a challenge. According to the Department of the Treasury, current financial statutes and regulations may not address new technology and evolving business models.[27] Regulators should create an agile framework that encourages innovation and sound risk management practices.[28] The FDIC Chairman has stated that:

> In many cases, the cost to innovation is prohibitively high for community banks, which often lack the expertise, information technology, and research and development budgets to independent[ly] develop and deploy their own technology . . . [I]f our regulatory framework does not evolve with technological advances in a manner that enables partnerships between banks and fintechs, such innovation may not occur at community banks.[29]

Further, bank examiners need up-to-date examination procedures to effectively assess the risks associated with new financial technologies.

The FDIC also faces challenges in issuing timely guidance that is consistent with other Federal banking regulators.[30] The Board of Governors of the Federal Reserve System, the OCC, the Consumer Financial Protection Bureau, and the FDIC share responsibility for Federal banking regulation and supervision.[31] These regulatory agencies work through the Federal Financial

---

[25] Washington Post, *Facebook's Zuckerberg takes broad lashing on Libra, 2020 election and civil rights at congressional hearing,* (October 23, 2019). See Commodity Futures Trading Corporation, *Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets*, (January 4, 2018), "US Law does not provide for direct, comprehensive Federal oversight of underlying Bitcoin or virtual currency spot markets." US regulation includes (1) the Internal Revenue Service treating virtual currencies as property subject to capital gains tax, (2) the Department of the Treasury Financial Crimes Enforcement Network monitoring virtual currency exchanges as money transmitters for anti-money laundering purposes, and (3) the Securities and Exchange Commission treating virtual currency issuances as securities issuances.

[26] CNBC, *JP Morgan Is Rolling Out the First US Bank-backed Cryptocurrency to Transform Payments Business*, (February 14, 2019). Reuters*, Wells Fargo Tests Cryptocurrency for Internal Transactions*, (September 17, 2019).

[27] Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, (July 2018).

[28] Jelena McWilliams, FDIC Chairman, Remarks at the Institute of International Bankers' Annual Washington Conference; Washington, D.C., (March 11, 2019).

[29] Statement of Jelena McWilliams, FDIC Chairman, on *Oversight of Financial Regulators* before the United States Senate Committee on Banking, Housing, and Urban Affairs, (December 5, 2019).

[30] American Banker, *Regulators Must Issue AI Guidance or FDIC Will: McWilliams*, (August 2, 2019); and American Banker, *Blockchain crypto tech need clear rules of the road*, (August 7, 2019).

[31] Jelena McWilliams, FDIC Chairman, "*Principles of Supervision and Your Value to our Nation's Banking System,"* delivered at the Banking Institute sponsored by the University of North Carolina School of Law; Charlotte, North Carolina, (March 21, 2019).

Institutions Examination Council (FFIEC)[32] to promote uniformity in the supervision of financial institutions. FDIC Chairman McWilliams recently noted her concern about the time required for regulators to reach consensus on artificial intelligence guidance and indicated that the FDIC may choose to issue its own guidance if regulators cannot agree on joint guidance.[33]

In October 2018, the FDIC announced the development of a new FDIC Tech Lab to centralize the FDIC's knowledge of technology in order to focus on technologies in the financial services sector, help the FDIC understand how innovation can contribute to the expansion of banking services, and promote the adoption of technology. As of January 2020, the FDIC continued to implement the operational foundation for the Tech Lab, including developing governing policies and procedures and searching for a Chief Innovation Officer to lead this effort.[34] In addition, the FDIC is seeking a range of other technologists—including data scientists, process engineers, software developers, and network security experts—to join the agency.[35] We are monitoring the FDIC's progress in standing up the Tech Lab.

Ensuring Examinations Identify and Mitigate Technology Risks

According to the *Interagency Guidelines Establishing Information Security Standards,*[36] a financial institution is responsible for the cybersecurity of its own information technology (IT) systems. Similarly, responsibility for compliance with consumer protection laws and regulations lies with the financial institution, regardless of whether the institution or a third-party service provider controls the information.[37] The FDIC assesses whether bank management has appropriate controls in place to mitigate cybersecurity risks and enhance consumer protections.

According to the OCC, bank examiners note that "the most common specific control deficiencies" at banks relate to: Patch Management, Network Configuration, and Access Management.[38] In addition, banks and service providers report that some of the common attacks against institutions include: Phishing incidents; Compromised credentials; and Automated Teller Machine exploits.

Since 2016, the FDIC has used the Information Technology Risk Examination (InTREX) work program to conduct bank IT examinations and assess financial institutions' management of third-party service providers. The FDIC developed InTREX to enhance IT supervision by providing examiners with risk-focused examination procedures.[39] Examiners use work programs to observe and document processes, and test controls. The FDIC may undertake

---

[32] 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.

[33] *Regulators Must Issue AI Guidance or FDIC Will: McWilliams*, American Banker, (August 2, 2019). There is also a need for regulatory clarity for blockchain and cryptocurrency. *See Blockchain crypto tech need clear rules of the road*, American Banker, (August 7, 2019)

[34] American Banker, *FDIC Chairman, Regulators Need New Approach to Innovation*, (October 4, 2019).

[35] American Banker, *FDIC Chairman, Regulators Need New Approach to Innovation*, (October 4, 2019).

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

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

[38] OCC, *Semiannual Risk Perspective*, (Fall 2019).

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

enforcement actions when examiners identify IT risks and weak management practices at the institutions.

From 2016 to 2018, the FDIC conducted more than 3,000 IT examinations. Examiners establish the scope of an IT examination consistent with a bank's IT complexity and risk. For example, the IT examination scope could be larger if new technology has been introduced, a new material third-party technology service provider is added, or bank information security testing identified material deficiencies.

Banks have expanded their use of advanced technologies such as person-to-person payments, cloud computing, and blockchain. These developments increased the overall IT risk profile of the banking industry and the complexity of FDIC IT examination work. As a result, the FDIC has devoted an increasing number of examination hours to IT supervision. For example, according to FDIC data for IT examinations completed by the FDIC between January 2017 and August 2018, the average number of hours per examination increased 11 percent. For that same period, the average IT examination hours for FDIC-identified banks with the highest IT risk increased 46 percent.

The increase in IT examination hours has led to geographic examiner resource gaps requiring examiners from one region to supplement examiners in another region. For example, the New York Regional Office noted that it has shortages of examiners qualified to complete IT examinations and required the assistance from other Regional Offices. The FDIC has a nationwide IT On-The-Job training program to increase the pool of qualified examiners for intermediate and advanced examinations. We have ongoing work to evaluate the FDIC's process for allocating examination staff, including examiner IT subject-matter experts, to safety and soundness examinations. Also, we plan to conduct a review of the FDIC's InTREX examination program.

Mitigating Risks Associated With Third-Party Service Providers

According to the OCC, "[b]anks increasingly rely on third-party service providers for technology and other solutions to compete in a rapidly evolving financial marketplace."[40] In addition, "cyber crime and espionage increasingly target third-party service providers because of the potential to access multiple networks from a single point."[41] For example, in July 2019, an employee of a third-party provider of Capital One exploited a firewall and gained access to sensitive information for approximately 106 million U.S. and Canadian customers.[42]

The OCC also noted that banks are relying on the same pool of third-party service providers for critical services such as payments, transaction processing, and maintenance of sensitive information. "[C]onsolidation in the bank technology service provider industry has resulted in fewer entities providing certain critical services."[43] Thus, if one third-party provider experiences a service disruption, operations at many banks may be affected.

The FDIC—through its supervisory examination processes—evaluates banks' monitoring of the security programs of their third-party providers. Bank management must exercise due diligence before entering into third party relationships. Due diligence includes, for example,

[40] OCC, *Semiannual Risk Perspective*, (Fall 2019).
[41] OCC, *Semiannual Risk Perspective*, (Spring 2019).
[42] CyberScoop, *Capital One is a cautionary tale for companies rushing to embrace new tech*, (July 31, 2019).
[43] OCC, *Semiannual Risk Perspective*, (Fall 2019).

understanding the third-party's risk and security controls, and ensuring clear lines of responsibility between the third-party and the bank on actions to be taken in the case of an incident. According to *Banking Technology Vision 2019* by Accenture, 69 percent of 784 banking and IT executives surveyed did not know about the security at their third-party service providers.[44] We plan to conduct a review to assess whether FDIC examination processes evaluate institutions' monitoring and management of risks associated with third-party relationships.

The FDIC should understand risks associated with emerging technology to provide banks with implementation guidance that balances banking sector safeguards with innovation. The FDIC should also ensure that examinations effectively address technology risks.

2| ENHANCING THE FDIC'S INFORMATION TECHNOLOGY SECURITY PROGRAM

The FDIC continues to increase its reliance on IT systems to fulfill its mission. As of June 2018, the FDIC had 338 IT systems that collect, store, or process Personally Identifiable Information (PII) and sensitive information. A total of 174 of the FDIC's 338 IT systems contained what the Agency has determined to be "sensitive PII." Further, the FDIC has legacy systems that are becoming difficult and expensive to maintain. The FDIC is in the process of modernizing its technology and must maintain the security of information within its systems as the IT environment evolves.

According to the Office of Management and Budget (OMB), the Federal Government is a significant target of cyberattacks, and in Fiscal Year 2018, Federal agencies experienced 31,107 cybersecurity incidents.[45] A recent report issued by the data protection firm, Veritas, stated that "ransomware damage costs will reach $20 billion by 2021."[46] Nearly 30 percent of Federal agency respondents to the Veritas survey had been directly affected by ransomware attacks in the past 3 years, and 80 percent of Federal respondents believed that ransomware and malware will be as great a concern—if not a greater concern—within the next 12 months. The report further noted that ransomware attacks at Federal agencies present risks to national security, employee productivity loss, prolonged loss of services, and loss of institutional trust. The Director of the Cybersecurity and Infrastructure Security Agency (CISA)[47] at the Department of Homeland Security (DHS) noted that ransomware attacks are "only getting worse."[48] The actors are shifting their business models and going to more coordinated attacks.

Also, in June 2019, a Senate Committee on Homeland Security and Governmental Affairs report[49] found that Federal agencies failed to comply with basic cybersecurity standards,

---

[44] Accenture, *Banking Technology Vision 2019, (May 7, 2019)*.
[45] *Federal Information Security Modernization Act of 2014 Annual Report to Congress,* (August 2019).
[46] Veritas, *Ransomware Threats Is Your Agency Ready?*, (December 2019).
[47] On November 16, 2018, the President signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018 (Act). The Act established the Cybersecurity and Infrastructure Security Agency (CISA) within the DHS to, among other things, make the United States cyber and physical infrastructure more secure by sharing information at all levels of Government and the private and non-profit sectors. Cybersecurity and Infrastructure Security Act of 2017, House Report 115-454, 115th Congress, (December 11, 2017).
[48] FedScoop, *Survey Indicates Federal Agencies Lack Adequate Planning to Recover from Ransomware Attacks*, (December 6, 2019).
[49] *Federal Cybersecurity: America's Data At Risk*, United States Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, (June 2019). The Subcommittee reviewed the

including deficiencies related to:

- Protecting PII;[50]
- Maintaining comprehensive and accurate lists of IT assets;
- Installing required security patches; and
- Ensuring systems had valid operating authorities.

This Senate Report also noted that agencies were at increased risk when they rely on aging systems also called "legacy systems."[51] These legacy IT systems are difficult to secure and costly to maintain.

FDIC IT systems reflect a combination of legacy systems and new technologies. According to the Government Accountability Office (GAO), use of legacy systems increases the cybersecurity risk of those systems.[52] Further, the FDIC's Chief Information Officer Organization recognized that the "burden of maintaining the legacy environment limits the ability of staff to develop and practice new skills and pursue innovation."[53]

The FDIC relies heavily on IT systems to carry out its responsibilities of insuring deposits, supervising banks, and performing its resolution and receivership activities. The FDIC maintains 338 IT systems that collect, store, or process PII and sensitive information. A total of 174 of the FDIC's 338 IT systems contain what the agency has determined to be "sensitive PII."[54] For example, in its capacity as receiver for failed banks, the FDIC collects and maintains a significant volume of PII such as names, home addresses, SSNs, dates and places of birth, bank account numbers, and credit card information. The FDIC also maintains business proprietary information that is sensitive, including banks' information relating to internal operations regarding counterparties, vendors, suppliers, and contractors.

In December 2019, the FDIC Chairman announced the departure of the Chief Information Officer (CIO) who led the FDIC's IT strategic planning and modernization efforts. On January 16, 2020 the Chairman named the Deputy CIO as the new CIO to continue leadership of the implementation of the FDIC's IT Modernization Plan. The appointment of the new CIO marks the FDIC's eighth CIO or Acting CIO in the last decade. These senior management changes impact the direction of an organization because turnover affects management strategy, planning, budgets, and staffing. As noted by the GAO, a high turnover rate in CIOs negatively

---

Department of Homeland Security, the Department of State, the Department of Transportation, the Department of Housing and Urban Development, the Department of Agriculture, the Department of Health and Human Services, the Department of Education, and the Social Security Administration.

[50] 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 (SSN), 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.

[51] U.S. Government Accountability Office, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471, (June 2019).

[52] U.S. Government Accountability Office, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471, (June 2019).

[53] FDIC Chief Information Officer Organization, *FDIC IT Modernization Plan 2020-2024*.

[54] According to FDIC Circular 1360.9, *Protecting Sensitive Information*, (October 2015), sensitive PII is a subset of PII that presents the highest risk of being misused for identity theft or fraud. Sensitive PII may be comprised of a single item of information, such as an SSN, or a combination of two or more items, such as full name along with financial, medical, criminal, or employment information.

impacts their effectiveness because there is limited time to put their agenda in place or form close working relationships with agency leadership.[55]

Maturing the FDIC's IT Security Program and Practices

In our annual audit report, *The FDIC's Information Security Program—2019* (October 2019) (FISMA Report) and other OIG reports, we identified 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. In particular, we identified the following weaknesses and deficiencies that pose the highest risks to FDIC IT systems:

- **Network Firewalls**. According to the National Institute of Standards and Technology (NIST) guidance, firewalls are essential devices or programs that help organizations protect their networks and information systems from hostile attacks, break-ins, and malicious software.[56] The FDIC deploys firewalls at both the perimeter and interior of its network. These firewalls control the flow of inbound traffic from the internet through the use of "ingress" rules that inspect traffic and permit or deny requests for access to FDIC systems. The firewalls also control the type of traffic allowed to flow out of the network using "egress" rules. Therefore, the FDIC's firewalls are only as effective as the rules that the FDIC defines for them.

  In our audit report, *Preventing and Detecting Cyber Threats* (May 2019), we identified weaknesses in the effectiveness of both FDIC firewalls and the Security Information and Event Management tool that works in concert with firewalls to analyze network activity and detect cyber threats. The FDIC had inadequate firewall policies and procedures that led to firewall rules lacking documented justification, unnecessary firewall rules, and an ineffective process to periodically review firewall rules. Unnecessary firewall rules pose a security risk. The FDIC undertook significant steps to address these network firewall weaknesses. However, the FDIC had not yet completed actions to document all existing network firewall rules with an approval and mission/business need, including the duration of that need, or implemented a firewall policy consistent with NIST guidance.

- **Privileged Account Management.** The FDIC assigns certain network users "administrative accounts" that have privileged access to systems and network IT resources to perform maintenance and IT troubleshooting activities. The FDIC must carefully control and monitor administrative accounts because hackers and other adversaries often target them to perform malicious activity, such as exfiltrating sensitive information.

  In our audit report, *Preventing and Detecting Cyber Threats*, we found that the FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls. These vulnerabilities exposed the network firewalls to increased risk of unauthorized access or malicious activity. The FDIC corrected these vulnerabilities.

- **Security Control Assessments.** Agencies are required to test and evaluate information security controls periodically in order to ensure that they are effective. The

[55] U.S. Government Accountability Office, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823, (July 2004).
[56] NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, (September 2009).

FDIC assessed its security controls following a risk-based schedule. However, in our audit, *Security Configuration Management of the Windows Server Operating System* (January 2019), we found instances in which security control assessors did not test the implementation of security controls, when warranted. Instead, assessors relied on narrative descriptions of controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls. We made eight recommendations, one of which remains unimplemented at the time of this report.

- **Security and Privacy Awareness Training.** FDIC policy requires employees and contractor personnel with network access to complete security and privacy awareness training within one week of employment, and annually thereafter. FDIC policy states that users who fail to comply with this requirement must have their network access revoked. We identified 29 network users who did not satisfy the FDIC's awareness training requirement but still had access to the network. We found that the FDIC was not aware of the 29 users, among approximately 7,000 network users, because the system used to monitor training compliance did not track all users required to take the annual security and privacy awareness training.

The FDIC must continue to modernize its IT systems and mature security controls to minimize risks of cyber incidents. Information security should remain a critical element of the FDIC's plan to modernize its IT systems.

3| ENSURING THE FDIC'S READINESS FOR CRISES

Banks face numerous significant risks that could affect the stability of the financial system, as well as the safety and soundness of institutions. Central to the FDIC's mission is readiness to address crises impacting the banking system and mitigation of risk through supervision. The FDIC identified two important lessons learned following the recent financial crisis: (i) the importance of crisis readiness planning; and (ii) quickly addressing emerging supervisory risks. Crisis readiness best practices identify the principles and elements of effective preparedness that collectively provide a framework for crisis planning efforts. Adopting such a framework strengthens the FDIC's ability to respond to a crisis in a timely and effective manner.

The World Economic Forum identified five categories of risk to the world economy that also impact the banking sector: (1) Technological risks, such as widespread economic disruption, failure of the internet or satellites, or large-scale data fraud or theft; (2) Economic risks, such as unsustainable prices for housing or commodities that result in sudden price drops; (3) Environmental risks, such as extreme weather events, natural disasters, or man-made disasters; (4) Geopolitical events, such as terrorist attacks or weapons of mass destruction; and (5) Societal risks, such as infectious disease pandemics.[57]

The FDIC plays an important role in supervising and regulating banks that may be affected by these risks. The FDIC helps to stabilize financial markets through its examination of banks, provision of deposit insurance, and resolution of failed banks. When the FDIC acts as the receiver of a failed institution, the FDIC assumes responsibility for recovering funds through the disposition of a bank's assets.[58] The FDIC Chairman noted that during its 85-year history, the

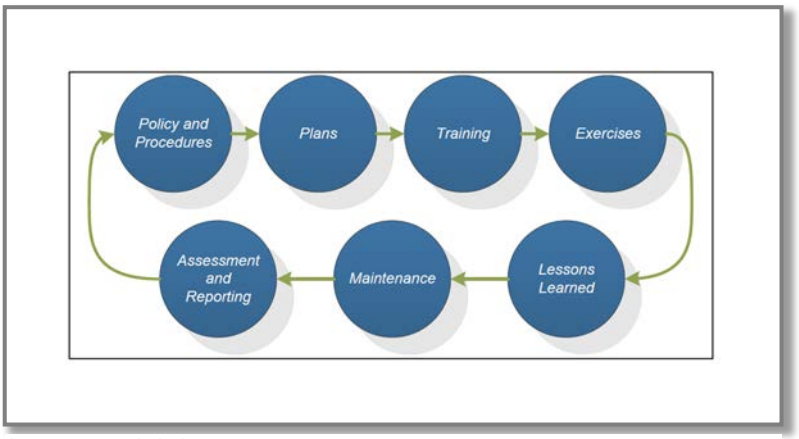
[57] The World Economic Forum, *The Global Risks Report 2018*, 13th Edition.
[58] FDIC 2018-2023 Strategic Plan, Receivership Management Program.

FDIC "has resolved more than 2,700 institutions with assets of more than $1 trillion and almost $800 billion in deposits."[59]

Planning for Crises and Resolution of Failed Banks

When early mitigation fails or events overtake mitigation efforts, the FDIC should be prepared to address bank failures. In 2017, the FDIC published a study of the Agency's response to the financial crisis in 2008-2013. The FDIC study, *Crisis and Response: An FDIC History, 2008-2013* (Crisis and Response Report), concluded that the financial crisis presented the FDIC with unprecedented challenges and demanded creative and innovative responses from the FDIC and other financial regulatory agencies. In addition, the crisis stretched the limits of the FDIC's capacity to supervise problem institutions, manage the Deposit Insurance Fund, and implement orderly resolutions for failed financial institutions. The Crisis and Response Report concluded that "[i]n hindsight, it might have been more effective if the FDIC, as part of its readiness planning, had built a larger and more agile infrastructure—including staff, contracts, and [information technology] systems—during the lull between the end of the previous crisis and the start of this new one." The Crisis and Response Report indicated that, as a result, one of the most important lessons learned from the prior financial crisis was that "readiness planning is essential."[60]

Figure 1: OIG Compilation of Crisis Readiness Framework



Source: FDIC OIG.

Crisis readiness best practices[61] identify seven elements of a readiness planning framework, as depicted in Figure 1. A crisis readiness framework identifies the principles and elements of effective preparedness and promotes a shared understanding and a common, integrated perspective of readiness across all mission areas.[62]

Specifically, the seven elements of a readiness framework that agencies such as the FDIC should have include:

- **Policy and Procedures –** Agencies should have a policy with defined readiness authorities, roles, and responsibilities, including a committee responsible for overseeing

[59] Jelena McWilliams, FDIC Chairman, Keynote Remarks delivered at the 2018 Annual Conference of The Clearing House and Bank Policy Institute, (November 28, 2018).
[60] The Crisis and Response Report indicated that, as part of maintaining readiness in a stable environment, the FDIC could explore how other agencies with highly variable resource demands address their resource challenges. The report cited FEMA as an example, noting the agency has developed readiness capabilities despite the unpredictable need for disaster relief.
[61] OIG-identified best practices included the Department of Homeland Security, *National Preparedness Guidelines* (September 2007); Federal Emergency Management Agency (FEMA), *FEMA Operational Planning Manual* (FEMA-P-1017) (June 2014); and the Organization for Economic Co-operation and Development, *Strategic Crisis Management* (December 2012).
[62] FEMA, *National Disaster Recovery Framework* website summary page https://www.fema.gov/national-disaster-recovery-framework (October 2018).

readiness activities. This policy helps ensure that personnel understand and implement management directives for readiness. Agencies should also have procedures for a consistent crisis readiness planning process.

- **Plans –** Agencies should have an agency-wide all-hazards readiness plan as well as plans for specific hazards as needed based on risk. These plans improve the efficiency of the readiness planning process and provide management and personnel with a comprehensive understanding of readiness planning activities across an organization.

- **Training –** Agencies' plans should incorporate training requirements to ensure that personnel understand the content of crisis readiness plans, including the task-related responsibilities for executing the plans.

- **Exercises –** Agencies should regularly test readiness plans, document the results of all readiness plan exercises, and consistently incorporate such exercise requirements within its plans.

- **Lessons Learned –** Agencies should have a process to monitor the implementation of lessons learned and related recommendations from readiness plan training, exercises and execution during a crisis.

- **Maintenance –** Agencies should regularly review and update their readiness plans and incorporate such maintenance requirements within their plans.

- **Assessment and Reporting –** Agencies should regularly assess and report on Agency-wide progress on crisis readiness plans and activities to key decision makers within an organization.

We have work ongoing to assess the FDIC's crisis readiness planning efforts in the context of this framework.

Promptly Identifying and Mitigating Banking Risks

An important step in avoiding crises is early risk identification and mitigation. In its review of the financial crisis, the Financial Crisis Inquiry Commission stated that "[i]n case after case after case, regulators continued to rate the institutions they oversaw as safe and sound even in the face of mounting troubles, often downgrading them just before their collapse."[63]

The FDIC adopted a Forward-Looking Supervision initiative to identify and mitigate risk before it impacts the financial condition of an institution. In our evaluation report, *Forward-Looking Supervision*[64] (August 2018) we found that for 41 examination reports sampled, examiners identified overall safety and soundness risk; however, only 27 percent of reports sampled (11 of 41) elevated concerns to the financial institution's board of directors. Based on the financial institutions' risk, we believe that a greater number of these concerns warranted board attention. Elevating concerns and recommendations provides greater visibility and awareness to the financial institution's board of directors and senior management.

[63] Financial Crisis Inquiry Commission, *Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United State*s (January 21, 2011). Congress established the Financial Crisis Inquiry Commission as part of the Fraud Enforcement and Recovery Act (Public Law 111-21) to examine the causes of the financial crisis.
[64] *Forward-Looking Supervision*, EVAL-18-004, (August 2018).

An institution's financial condition may also change between examination intervals, making the most recent examination rating outdated or inaccurate. The FDIC's Offsite Review Program (ORP) is designed for the early identification of emerging supervisory concerns and potential problems so that supervisory strategies can be adjusted quickly. The ORP includes models and other methodologies that review quarterly bank information[65] and produce the Offsite Review List (ORL) of institutions with potential emerging supervisory concerns. FDIC Regional Offices may add institutions that are not initially identified on the ORL based on Region-specific concerns. The ORP also includes a Supplemental Review List for new or emerging risks to be included in the quarterly offsite process.

In our evaluation report, *Offsite Reviews of 1- and 2-Rated Institutions* (December 2019), we found that the ORP identified emerging issues concerning financial institutions' rapid growth, use of noncore funding, and deteriorating financial trends, but the FDIC should evaluate additional methods and new technologies to identify financial institutions with other types of emerging supervisory concerns. For example, the FDIC should assess whether innovative technologies would provide predictive information on other types of emerging supervisory concerns, such as those related to banks' internal controls, credit administration, and management practices. We recommended that the FDIC evaluate the feasibility of using new technologies to identify institutions with emerging supervisory concerns.

The health of banks and the banking system depends upon the FDIC's and other regulators' early identification and mitigation of safety and soundness risk and the FDIC's ability to respond to banking crises. Establishing a robust readiness framework ensures the FDIC has the organizational processes, individuals, resources, and integration necessary to respond to a crisis.

4|SHARING THREAT INFORMATION WITH BANKS AND EXAMINERS

Federal Government agencies gather a substantial volume of information related to the safety and soundness of financial institutions in the United States, and thus, relevant to FDIC supervisory activities. For example, Government agencies collect information about cyber threats, money laundering, and illicit financing activity. Bankers need to receive actionable information in order to respond to threats in a timely manner. FDIC examiners responsible for supervised institutions should be aware of threats directed toward those institutions to understand their impact and make necessary supervisory adjustments. Further, examiners should understand the nature of threats to evaluate potential gaps and determine the depth and scope of an examination. FDIC policy makers should be aware of emerging threats to ensure that relevant threat information is disseminated to banks and examiners; in addition, policy makers can adjust examination policy and procedures and assess the need for supplementing or modifying the regulatory scheme.

On April 30, 2019, the CISA identified consumer and commercial banking, and funding and liquidity services as National Critical Functions which are "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[66] The CISA

[65] Banks reviewed through the ORP include FDIC-supervised institutions and institutions supervised by the Federal Reserve Board or the Office of the Comptroller of the Currency.
[66] DHS Cybersecurity and Infrastructure Security Agency, *National Critical Functions – An Evolved Lens for Critical Infrastructure and Security Resilience*, (April 30, 2019).

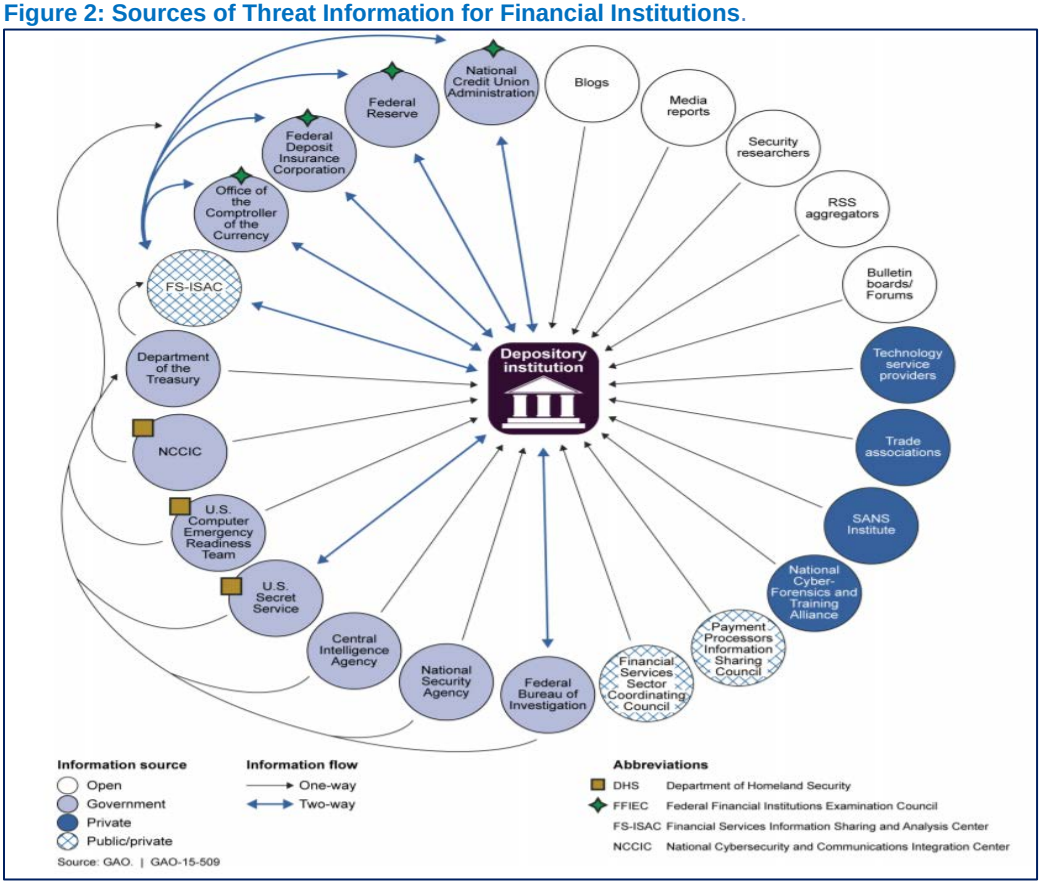
further stated that a key focus to support these National Critical Functions is collecting and sharing threat information about natural occurrences or man-made actions that represent "the potential to harm life, information, operations, the environment, and/or property."[67]

Similarly, the FSOC noted, in its 2019 Annual Report, the critical importance to the financial sector of sharing timely and actionable threat information with Federal Government agencies and the private sector. The FSOC stated that Federal agencies should "carefully consider how to appropriately share information and, where possible, continue efforts to declassify (or downgrade classification) to the extent practicable, consistent with national security imperatives."[68]

FinCEN also stressed the importance of providing the financial sector with information about illicit activity to help sector participants identify and report such activities to law enforcement.[69] This information is especially important to identify illicit actors who use virtual currency to facilitate criminal activity, such as human or drug trafficking, child exploitation, fraud, terrorist financing, or to support rogue regimes and facilitate sanctions evasion.

As shown in Figure 2, the GAO identified multiple sources of threat information.

Figure 2: Sources of Threat Information for Financial Institutions.



[67] Department of Homeland Security, *DHS Risk Lexicon*, (September 2008).
[68] FSOC 2019 Annual Report.
[69] Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency,* (May 9, 2019).

Disseminating Threat Information to Banks

The OCC noted that "[t]he potential for operational disruptions underscores the need for effective controls and operational resilience to help ensure the ongoing delivery of financial products and services in a safe and sound manner."[70] The FFIEC provides instructions to examiners on how to examine financial institutions' business continuity plans. These instructions note that threats should be analyzed "based upon the impact to the institution, its customers, and the financial market it serves."[71] 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." The FDIC is responsible for evaluating bank management's processes to receive and assess threat information, and to act on such information in order to mitigate risks.

The Cybersecurity Information Sharing Act (2015) required the Director of National Intelligence (DNI) and other agency heads to develop and issue procedures to facilitate and promote the sharing of cyber threat indicators and defensive measures. In February 2016, the DNI issued a report entitled *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015* (Threat Sharing Procedures), which outlined the procedures for Federal agencies to share cybersecurity information with non-Federal entities such as financial institutions.[72] The Threat Sharing Procedures promote sharing unclassified and classified information, and best practices related to cyber security.

According to the Threat Sharing Procedures, Federal Government agencies are to make every reasonable effort to share unclassified reports of cyber threats on a timely basis. The sharing of classified threat information is dependent on the recipient's security clearance level and must protect sources, methods, operations, and investigations. The Threat Sharing Procedures encourage Federal agencies to "downgrade, declassify, sanitize or make use of tearlines to ensure dissemination of threat information to the maximum extent possible."[73]

Federal agencies may use Information Sharing and Analysis Centers (ISAC) to provide threat information to other government agencies or non-Federal entities.[74] The goal of ISACs is to provide members with accurate, actionable, and relevant information, and they are organized to share sector-specific threat and vulnerability information with members.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established to serve financial institutions. FS-ISAC has 7,000 members and its purpose is to share timely, relevant, and actionable security threat information. Federal financial-sector regulators encourage financial institutions to gain access to threat information through FS-ISAC membership.[75] Regulators also suggest that banks use other available resources from the Federal Bureau of Investigation, Department of Homeland Security, and U.S. Secret Service in

[70] OCC, *Semiannual Risk Perspective*, (Fall 2019).
[71] FFIEC, Business Continuity Planning Booklet, *Risk Assessment*, (Available on the FFIEC website).
[72] The Office of the Director of National Intelligence, The Department of Homeland Security, The Department of Defense, and The Department of Justice, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015,* (February 16, 2016).
[73] The Office of the Director of National Intelligence, The Department of Homeland Security, The Department of Defense, and The Department of Justice, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015,* (February 16, 2016).
[74] Presidential Policy Directive 63, *Critical Infrastructure Protection*, (May 22, 1998).
[75] FFIEC, *Cybersecurity and Threat and Vulnerability Monitoring and Sharing Statement*, (November 3, 2014).

order to identify and respond to cyber attacks. Bank "management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly."[76]

As part of the FDIC's supervisory process, examiners evaluate banks' processes for obtaining and assessing threat information. Examiners may face challenges in assessing the effectiveness of banks' threat identification and mitigation processes when banks are not receiving threat information through FS-ISAC membership.

Disseminating Threat Information to FDIC Policy Makers and Examiners

FDIC policy makers should be aware of threats to ensure relevant threat information is provided to banks and examiners. Further, policy makers may need to adjust examination policy and procedures to address emerging threat issues and assess the need for additional regulation. FDIC examiners should be aware of threats directed toward those institutions to understand their impact and make necessary supervisory adjustments. Understanding the nature of threats to all banks provides context for examiners to evaluate potential gaps in an institution's processes for threat information gathering and continuity planning. Further, threat information can assist examiners in prioritizing and focusing their work on emerging issues, and modifying the depth or scope of an examination.

According to best practices,[77] recipients of threat information should have the following processes in place to assess the significance of the information and ensure that actionable information is disseminated to relevant parties:

- **Acquiring Threat information.** Threat information may be obtained from a variety of sources and methods, including information from open sources, confidential sources, law enforcement, intelligence, public and private entities, as well as investigations, assessments, and intelligence collection.

- **Analyzing Threat Information.** The significance of the threat must be assessed in the context of other threats and relevant information.

- **Disseminating and Using Actionable Threat Information.** This step includes distribution with a focus on timely delivery of relevant actionable threat information to the appropriate people. Further, information must be "marked" to ensure proper safeguarding and access restrictions.

- **Providing Feedback on Threat information.** Establishing processes for lessons learned improves the relevance, usefulness, and format of threat information.

The FDIC has access to threat information held by various Government agencies, and should have formal processes to address the four steps, referenced above, for threat information assessment and sharing. Without formal processes, the FDIC leaves the collection of information, analysis, dissemination, and feedback to staff discretion, which may lead to inconsistencies, uncertainty, and a lack of uniformity in sharing threat information.

---

[76] FFIEC, *Cybersecurity and Threat and Vulnerability Monitoring and Sharing Statement*, (November 3, 2014).
[77] OIG compilation based on a combination of DHS, *Critical Infrastructure Threat Information Sharing Framework, A Reference Guide for the Critical Infrastructure Community*, (October 2016); and SANS Institute, *Cyber Threat intelligence Support to Incident Handling*, (November 2017).

The FDIC is also challenged to set up the infrastructure needed to execute threat assessment and sharing processes. 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. Given the volume of information, the FDIC faces challenges in having the appropriate number of personnel with the requisite security clearance levels to analyze, distill, and convey relevant and actionable threat information. The FDIC is also challenged to convey classified information to policy makers and examiners. In order to access, store, and handle classified information, FDIC policy makers and examiners must have relevant security clearances and secure facilities—or alternatively, the FDIC must have processes in place to declassify information in a timely manner. We have ongoing work to evaluate the effectiveness of the FDIC's procedures for the collection and dissemination of threat information.

Timely and actionable threat information allows bank management to thwart threats and the FDIC to quickly adjust supervisory strategies. Understanding the emerging threat landscape across all banks provides examiners with context to review a bank's processes to defend against threats and provides perspective to adjust examination policies and procedures. Absent information sharing, bank management, policy makers, and examiners may be unaware of threats that could affect the safety and soundness of financial institutions.

5| STRENGTHENING THE GOVERNANCE OF THE FDIC

Effective governance is critical to ensure proper oversight of the FDIC. The Federal Deposit Insurance Act vests the management of the FDIC to its Board of Directors (FDIC Board). The FDIC Board has operated without a full membership since 2015. The FDIC Board delegates authority to FDIC senior leaders to fulfill the Agency's mission, including implementation of its Enterprise Risk Management (ERM) program. The FDIC should ensure that it is identifying and managing risks, and making data-driven acquisition decisions.

According to *Principles of Corporate Governance* issued by the Organization for Economic Co-operation and Development (OECD Governance Principles), "[t]he purpose of corporate governance is to help build an environment of trust, transparency and accountability necessary for fostering long-term investment, financial stability, and business integrity, thereby supporting stronger growth, and more inclusive societies."[78] As explained in the OECD Governance Principles, a governance framework should ensure strategic guidance, effective monitoring of management by the board, and the board's accountability to stakeholders.

One area of importance for boards is oversight of the organization's ERM. Such oversight includes accountability and responsibilities for managing risks, specifying the types and degree of risk that an organization is willing to tolerate, and the management of risks through operations and relationships. ERM is a governance issue that falls within the oversight responsibility of boards of directors.[79]

[78] OECD, *G20/OECD Principles of Corporate Governance*, (2015). *The Principles* are presented in six different chapters. This document references two chapters: (1) Ensuring the basis for an effective corporate governance framework and (2) The responsibilities of the Board.
[79] Harvard Law School Forum on Corporate Governance and Financial Regulation, *Risk Management and the Board of Directors*, (March 20, 2018).

The Federal Deposit Insurance Act[80] vests management of the FDIC in the FDIC Board. The FDIC Board consists of five members, all of whom are appointed by the President and confirmed by the Senate: the Comptroller of the Currency; the Director of the Consumer Financial Protection Bureau; and three "Appointive Directors," including a Chairman and Vice Chairman.[81] No more than three members of the Board may be from the same political party, and one member "shall have State bank supervisory experience."[82]

Although the FDIC Board may delegate certain powers to officers of the FDIC, the FDIC Board members should exercise oversight, remain informed about FDIC activities, and review financial statements.[83]

Maturing Enterprise Risk Management

According to OMB Circular Number A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*,[84] Federal agencies face internal and external risks to achieving their missions, including "economic, operational, and organizational change factors."[85] The OMB requires that Federal agencies implement ERM to assist agencies in identifying, assessing, and mitigating internal and external risks.

The OMB defines ERM as "an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos."[86] The components of ERM include a risk governance structure; a methodology for developing an agency's risk profile; and a process, guided by an organizations senior leadership, to consider risk appetite and risk tolerance levels that serve as a guide for the agency to establish strategy and select objectives.

In June 2010, the FDIC hired a consulting firm to address five key issues regarding its ERM program. In response to the firm's recommendations, the then-FDIC Chairman 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 Chief Risk Officer (CRO), with total staffing of 16. The Board approved the recommended changes, which were intended to provide an office to review internal and external 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.

From 2011 to 2016, the ERM program was headed by a CRO who reported directly to the then-Chairman. In May 2016, the CRO retired, and only five ERM program staff remained at the

---

[80] 12 U.S.C. § 1812(a)(1) (2019).
[81] 12 U.S.C. § 1812(a)(1) (2019); FDIC, *Bylaws of the FDIC*, (2018). Technically designated the Chairperson and Vice Chairperson in the statute and bylaws, it is longstanding FDIC practice to refer to the positions as Chairman and Vice Chairman.
[82] 12 U.S.C. § 1812(a)(1) (2019).
[83] Bylaws of the Federal Deposit Insurance Corporation, Adopted by the Board of Directors, (September 17, 2019); Wyoming Law Review, *Director Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron*, (2006).
[84] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, (July 15, 2016).
[85] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, (July 15, 2016).
[86] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (July 15, 2016).

time. In June 2017, the FDIC reorganized the ERM program by placing the positon of CRO under the Division of Finance as a Deputy Director, eliminating OCRM and moving the ERM function to a newly constituted Risk Management and Internal Controls Branch.

In October 2018, the FDIC revised its *Enterprise Risk Management and Internal Control Policy* (FDIC ERM Directive), which includes the ERM principles of OMB Circular Number A-123.[87] The FDIC ERM Directive vests the FDIC's Operating Committee with oversight of the ERM program, including "establishment of the agency's risk profile, regular assessment of risk, and development of appropriate risk response." [88] The Operating Committee includes senior-level officials, but it is not a decision-making body.

The FDIC ERM Directive instructs the CRO to work in partnership with FDIC Division and Office leaders to ensure enterprise-wide coordination, training, policy, and maintenance of ERM components (risk inventory, risk profile, and risk appetite statements). The FDIC ERM Directive states that implementation of ERM should facilitate efforts of the FDIC Board to identify, assess, and address risks. However, the FDIC ERM Directive does not envision an oversight role for the FDIC Board, nor does it describe regular reporting requirements or communications for the FDIC Board.

In our recent audit, *The FDIC's Information Security Program–2019* (October 2019), we found that the ERM program developed a risk appetite statement establishing the amount of risk the FDIC is willing to accept in pursuit of its mission. However, as of the time of our report, the FDIC had not yet completed an inventory of risks facing the FDIC, or a risk profile to help manage and prioritize risk mitigation activities.

Subsequent to our report, the FDIC completed a risk inventory and risk profile. FDIC management is in the process of integrating its ERM program into the FDIC's budget, strategic planning, performance reporting, and internal control processes. We have ongoing work evaluating 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.

Operating Without a Full FDIC Board

The FDIC Board has been operating with four members since 2015. The Vice Chairman position on the FDIC Board of Directors has been vacant since April 30, 2018.[89] In addition, the FDIC has not had an independent Board member with "State bank supervisory experience" since 2012.[90] Nearly 80 percent of banks in the United States (approximately 4,400 institutions) are chartered by states, and the FDIC has authority to examine and supervise state-chartered banks that are not part of the Federal Reserve System.

On January 30, 2019, a bipartisan group of fifteen Members of the House of Representatives submitted a letter to the White House expressing concern that no current sitting FDIC Board

[87] FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (2018). The FDIC is not required to follow OMB Circular No. A-123.
[88] FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (2018).
[89] American Banker, *Pressure Grows on Administration to Fill Fed, FDIC Seats*, (November 3, 2019).
[90] Former Comptroller of the Currency Thomas Curry, who served on the FDIC Board until May 2017, was formerly the Massachusetts Banking Commissioner, but did not meet the statutory requirement for an independent Board member with supervisory experience. See American Banker, *FDIC Needs a State Regulator on Its Board*, (August 17, 2018).

member satisfies the state banking supervisory experience requirement.[91] The Congressional Members noted in the letter that state bank supervisory experience is important because both state and FDIC regulators share concurrent responsibility for the safety and soundness of certain state-chartered banks. Most state banking agencies participate in an examination program under which certain examinations are performed on an alternating basis by the state agency and the FDIC. The Members of Congress stated they believe that "having an FDIC Board member with state bank experience is an important part of that coordination."

Overseeing Investment Decisions

In order to properly oversee investment decisions at the FDIC, the FDIC Board and senior managers should have quality data and processes. The FDIC awarded 2,400 contracts valued at more than $1.5 billion over a 3-year period from 2016 to 2018. In our evaluation report, *Contract Oversight Management* (October 2019), we found that the FDIC was overseeing acquisitions on a contract-by-contract basis rather than on a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. In addition, we found that the FDIC's contracting system did not maintain certain key data in a manner necessary to conduct historical trend analyses, plan for future acquisition decisions, and assess risk in the FDIC's awarded contract portfolio. As a result, FDIC Board members or other senior management officials were not provided with a portfolio-wide view or the ability to analyze historical contracting trends across the portfolio, identify anomalies, and perform ad hoc analyses to identify risk or plan for future acquisitions.

In our audit report, *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. The FDIC has taken action to address six of our eight recommendations and continues to work towards implementing the remaining two recommendations relating to: (1) revising IT Governance Processes into FDIC policies and procedures; and (2) identifying and documenting IT resources and expertise needed to execute the FDIC's IT Strategic Plan.

The FDIC Board's oversight of FDIC senior management is a critical component to promptly identifying, assessing, and responding to risks to the FDIC, and overseeing contracting activities and IT investment decisions.

[91] The letter is available here. Congressman Barry Loudermilk, Congressman Denny Heck, Congressman Peter King, Congressman Jim Hines, Congressman Frank Lucas, Congressman Scott Tipton, Congressman Tom Emmer, Congressman Steve Stivers, Congressman Lee Zeldin, Congressman Alex Mooney, Congressman Ted Budd, Congressman David Kustoff, Congressman Trey Hollingsworth, Congressman John Rose, and Congressman Denver Lee Riggleman III.

6|OVERSEEING HUMAN RESOURCES

The FDIC relies on the talents and skills of its employees to accomplish its mission. Within the next few years, the FDIC will need to navigate a potential wave of retirements, reverse attrition trends among its core examination workforce, and hire staff with skills to match technology innovation. Effective management of these challenges limits the impact of leadership and skill gaps, and the loss of institutional experience and knowledge due to retirements. The FDIC should position itself to recruit, retain, and develop future talent.

In March 2019, the GAO recognized strategic human capital management as a continuing Government-wide area of high risk.[92] The GAO noted that 31.6 percent of the permanent Federal workforce on board as of September 30, 2017 would be eligible to retire within the next 5 years.[93] The GAO identified the need for Federal agencies to measure and address existing mission-critical skill gaps, and to use workforce analytics to predict and mitigate future gaps.[94] The GAO also identified five trends affecting the future Government workforce:

(1) Technological advances that will change the way work is performed;
(2) Increased reliance on contractors to achieve policy goals that will require new skills and competencies;
(3) Fiscal constraints that will require agencies to review how they conduct business;
(4) Evolving mission requirements that will require agencies to adapt their work and workforce; and
(5) Changing demographics and shifting attitudes towards work.[95]

Without careful attention to strategic and workforce planning and other approaches to managing and engaging personnel, reduced investments in human capital may have lasting effects on the capacity of an agency's workforce to meet its mission.[96]

Forty-two percent of current FDIC employees (on board as of July 31, 2019) are eligible to retire within the next 5 years. These retirement figures include retirement eligibility of 60 percent for FDIC Executives and 58 percent for its Managers. Although historical FDIC projections show that employees may not retire on their eligibility date, this wave of potential retirements could deplete the FDIC's institutional experience and knowledge, especially during a crisis. Without proper succession planning strategies, these retirements can also result in leadership gaps.

Further, the FDIC's budget for 2019 marked the ninth consecutive year of lower annual staffing levels and operating budgets, reflecting the FDIC's reduced bank failure workload. The FDIC's authorized staffing level at the beginning of 2019 of 5,901 positions represented a net reduction of 182 positions from 2018 (approximately 3.1 percent) and the operating budget was reduced by 2.3 percent for the same period.

---

[92] GAO, High-Risk Series*: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 2019).
[93] GAO, *Federal Workforce: Talent Management Strategies to Help Agencies Better Compete in a Tight Labor Market*, GAO-19-723T, (September 2019).
[94] GAO, High-Risk Series*: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 2019).
[95] GAO, *Federal Workforce: Key Talent Management Strategies for Agencies to Better Meet Their Missions*, GAO-19-181, (March 2019).
[96] GAO, *Federal Workforce: Key Talent Management Strategies for Agencies to Better Meet Their Missions*, GAO-19-181, (March 2019).

Retirements and attrition can create opportunities for employees and allow organizations to restructure to meet program goals and fiscal realities. However, if turnover is not strategically monitored and managed, gaps can develop in an organization's institutional knowledge and leadership.[97]

Navigating the Upcoming Retirement Waves in the FDIC's Primary Divisions

Approximately 91 percent of all FDIC employees work in one of the FDIC's nine primary and support Divisions. We analyzed the data regarding eligibility for retirement of the employees within these Divisions as illustrated in Table A. Based on our review, we found that 30 to 67 percent of the FDIC staff in these Divisions is eligible to retire in the next 5 years. Notably, all but one of the primary FDIC Divisions have retirement eligibility rates that are higher than the Federal Government average of 31.6 percent.

FDIC Executives and Managers in the nine Divisions have retirement eligibility rates ranging from 29 to 76 percent. For example, more than three-quarters of FDIC Executives and Managers within the Division of Finance (76 percent) are eligible to retire in the next 5 years. Similarly, 70 percent of Executives and Managers in the Division of Resolutions and Receiverships can retire in the same timeframe.

The 5-year retirement rates of Executive Managers and Corporate Managers could result in knowledge and leadership gaps at the FDIC. As recognized by the GAO, retirement waves may result in leadership gaps.[98] These mission-critical skills gaps could impede the capabilities of any agency to achieve its mission, unnecessarily delay decision-making, and reduce program management and oversight.[99]

Table A: Retirement Eligibility Statistics for Key FDIC Divisions

Division	Staff Eligible to Retire in 2024	Executives and Managers Eligible to Retire in 2024
Division of Resolutions and Receiverships (DRR)	67 percent	70 percent
Division of Finance (DOF)	61 percent	76 percent
Legal Division	56 percent	44 percent
Division of Administration (DOA)	53 percent	57 percent
Division of Information Technology (DIT)	46 percent	52 percent
Division of Risk Management Supervision (RMS)	39 percent	63 percent
Division of Complex Institution Supervision & Resolutions (CISR)	35 percent	29 percent
Division of Depositor and Consumer Protection (DCP)	33 percent	51 percent
Division of Insurance and Research (DIR)	30 percent	39 percent

Source: OIG analysis of FDIC-provided data as of July 31, 2019.

[97] GAO, *Federal Workforce: Sustained Attention to Human Capital Leading Practices Can Help Improve Agency Performance*, GAO-17-627T, (May 2017).
[98] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317, (February 2017).
[99] Southern California Law Review, *Vacant Offices: Delays In Staffing Top Agency Positions*, (2008).

The FDIC faces significant risks regarding retirement eligibility in key Divisions involved in crises readiness efforts. For example, two-thirds of FDIC employees within DRR are eligible to retire by 2024. DRR staff is responsible for managing resolutions and receiverships when banks fail, including ensuring the prompt payment of deposit insurance funds to eligible bank customers. During the financial crisis, the FDIC had the benefit of experienced DRR employees. Absent seasoned employees with knowledge from past crises, the FDIC may not be sufficiently agile and could delay decisions and resolution determinations.

DOF, the Legal Division, DOA, and DIT also play important roles to support DRR in a crisis situation when banks fail. These Divisions also face 5-year staff retirement eligibility rates ranging from 46 to 61 percent. DOF staff manages the liquidity of the Deposit Insurance Fund to ensure that money is available to DRR to pay depositors quickly in the event of a bank failure, and attorneys in the Legal Division assist DRR in structuring resolution agreements. DOA staff provides contracting support for DRR, including, for example, the rapid hiring of temporary personnel to address crisis staffing requirements, and DIT provides IT support for necessary computers and servers during bank failures and crises.

A significant number of employees responsible for ensuring the safety and soundness of institutions and protecting consumers are also eligible to retire. Specifically, 39 percent of RMS staff is eligible to retire within 5 years, and more than 62 percent of its Executives and Managers may retire over the same period. CISR similarly addresses supervisory and resolution risks for banks with over $100 billion in assets. Staff in CISR has a 5-year retirement eligibility rate of 35 percent. In addition, DCP conducts examinations to ensure that banks meet certain requirements for consumer protection, anti-discrimination, and community reinvestment. Thirty-three percent of its staff is eligible to retire within 5 years, and 51 percent of its Executives and Managers may retire during this same timeframe. All supervision-related Divisions are supported by the banking-sector research and analysis performed by DIR, which has a retirement eligibility rate of 30 percent within the next 5 years.

The FDIC should continue to ensure that the institutional knowledge of retirement-eligible employees is captured and passed on to new employees. The FDIC has programs underway to review succession planning and we will monitor those efforts.

Navigating the Upcoming Retirement Wave in FDIC Regional Offices

The FDIC has six Regional Offices located throughout the country. Regional Offices include members from all FDIC Divisions, but the largest representation of employees is RMS examination staff. The FDIC faces risk due to staff retirement eligibility rates within each of its Regional Offices.

Similar to the above analysis regarding each of the FDIC Divisions, we also assessed the data regarding the eligibility for retirement of employees in the Regional Offices. Based on our analysis, as shown in Table B, we found that FDIC employees in these Regional Offices are eligible to retire in the next 5 years at rates ranging from 33 to 53 percent, and retirement rates for Executives and Managers range from 44 to 77 percent. For example, in the Dallas Regional Office alone, more than half of its staff is eligible to retire in the next 5 years, and more than three-quarters of its Executives and Managers can do the same.

Table B: Retirement Eligibility Statistics for FDIC Regional Offices

Region	Staff Eligible to Retire in 2024	Executives and Managers Eligible to Retire in 2024
Dallas	53 percent	77 percent
New York	40 percent	44 percent
Atlanta	39 percent	47 percent
San Francisco	37 percent	58 percent
Chicago	36 percent	60 percent
Kansas City	33 percent	74 percent

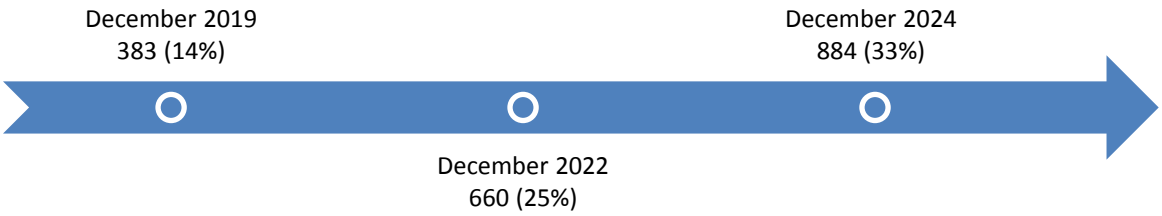
Source: OIG analysis of FDIC-provided data as of July 31, 2019.

Regional Office personnel are the critical interface between the FDIC and bank management. Regional Office examiners evaluate bank management's controls to maintain safety and soundness, mitigate cybersecurity risks, and minimize harm to consumers. Regional Office personnel also play a significant role during financial crises. The FDIC's Dallas Regional Office houses operational capabilities for large-scale bank failures, and it has among the highest rates of retirement eligibility at the FDIC.

Addressing Attrition Among FDIC Examiners

As of July 31, 2019, 47 percent of FDIC employees were classified as examiners. These examiners are deployed to four FDIC Divisions: RMS, DCP, DIR, and CISR, and to the FDIC's Corporate University.[100] As shown in Figure 3, at the end of 2019, 14 percent of examiners were eligible to retire. However, that number of retirement-eligible examiners jumps to 25 percent within 3 years (2022) and increases further to 33 percent (one-third of the examiner workforce) in 5 years (2024).

Figure 3: FDIC Examiner Retirement Eligibility



Source: OIG analysis of FDIC retirement data.

In addition, approximately 72 percent of all FDIC examiners are assigned to safety and soundness and IT examination positions within RMS. In 2018, 11 percent of RMS examiners resigned from their position, retired, or were promoted to non-examiners positions within the FDIC; this figure represents a 9-percent increase from the prior year. According to RMS surveys of managers of departing examiners, a significant portion of the attrition rate attributable to resigning examiners was dissatisfaction with the amount of travel required to conduct examinations. The FDIC has noted that safety and soundness examiners spent an average of 89 nights per year away from home, more than 24 percent of the year.[101]

[100] As of July 31, 2019, the FDIC's Corporate University had 142 employees training for examiner commissions. Examiners are assigned to Corporate University during their first year of training.
[101] Statement of Jelena McWilliams, FDIC Chairman, on *Oversight of Financial Regulators* before the United States Senate Committee on Banking, Housing, and Urban Affairs, (December 5, 2019).

Examiner attrition is costly. The FDIC invests an average of $620,000 per person to train new hires to become commissioned examiners over the period of 4 years (an average of approximately $155,000 annually per examiner).[102] Historically, entry-level employees hired for examination positions must progress through the FDIC's Corporate Employee Program (CEP) rotational year, be assigned to a Division, and then meet benchmarks, complete training, and meet technical requirements to become commissioned examiners.[103]

During the 4-year examiner pre-commissioning, the FDIC loses between 7 and 8 percent of participants each year at an average cost of about $1.3 million per year. For example, according to RMS statistics, for the five CEP cohorts from 5 years ago (the class of 2014), 35 percent of participants departed before completion of the 4-year commissioning process.

In August 2019, the FDIC announced changes to its approach for recruiting, hiring, and training examiners. The planned changes are aimed at improving the process for hiring new examiners and reducing the time for an examiner to attain commission by 6 to 8 months. We have ongoing work to evaluate the FDIC's allocation and retention of human capital for the examination function.

The FDIC should also align its human capital strategy to meet the challenges of rapidly changing bank technology. Community banking is increasingly dependent on a model that relies on technology provided by third-party partners, such as credit bureaus and payment networks, but it also includes new customer-facing and back-office collaborators.[104] The FDIC should have examination staff that understands new technology in order to examine risks.

The FDIC should take a strategic approach to align its human capital management with current and future mission requirements, including technology changes. Addressing human capital holistically from planning through retirement allows the FDIC to maximize performance and manage the waves of retirements and attrition.

7|KEEPING FDIC FACILITIES, INFORMATION, AND PERSONNEL SAFE AND SECURE

The FDIC is responsible for protecting approximately 6,000 employees and 3,000 contract personnel who work at 94 FDIC-owned or leased facilities throughout the country. The FDIC is also custodian of 338 systems containing sensitive information about banks and PII of employees, contractors, bank management, and bank deposit holders. A total of 174 of the FDIC's 338 IT systems contain what the agency deems to be "sensitive PII." The FDIC is challenged to have appropriate processes in place to safeguard facilities, information, and personnel.

According to the Worldwide Threat Assessment of the US Intelligence Community[105] (2018) (Threat Assessment), foreign intelligence agencies, terrorist groups, and criminal organizations strive to gain access to proprietary information from the finance industry and attempt to recruit sources such as trusted insiders.[106] According to Verizon's 2018 Data Breach Investigations

[102] Average costs per examiner are based on RMS calculations for the five cohorts of new hires for 2014.
[103] The FDIC is eliminating the CEP program in 2020.
[104] Accenture, *Banking Technology Vision 2019*. Governor Michelle W. Bowman, *Community Banking in the Age of Innovation,* at the "Fed Family" Luncheon at the Federal Reserve Bank of San Francisco, San Francisco, California, (April 11, 2019).
[105] Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community (February 13, 2018).
[106] Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community (February 13, 2018).

Report, one-third of all cyber breaches of government information is the result of privilege misuse and errors by insiders.[107] A Carnegie Mellon University paper entitled *Analytic Approaches to Detect Insider Threats* estimated the cost of an insider attack to be $445,000.[108] With an average of 3.8 insider attacks per organization per year across all industries, annual costs to an organization can reach $1.7 million.[109]

According to the GAO, a background investigation program should ensure the identification and assessment of individuals with criminal histories and questionable behavior.[110] Background investigations "minimize the risks of unauthorized disclosures of classified information and … help ensure that information about individuals with criminal histories or other questionable behavior is identified and assessed."[111]

Also, Federal managers and supervisors are responsible for assessing facility risk, assigning facility security levels, and determining whether implemented countermeasures effectively mitigate risk.[112] Further, Federal agencies must protect the PII and sensitive information they possess. PII includes 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 (SSN), 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. PII protection includes information contained in IT systems as well as other forms. In March 2019, the GAO identified the protection of privacy and sensitive data as a major challenge for the Federal Government.[113] As of June 2018, the FDIC reported that it maintained 338 information systems containing PII, including 174 systems that contain what the agency deems to be "sensitive PII."

Implementing Risk-Based Physical Security Management

The FDIC maintains 94 leased or owned facilities across the country that house approximately 9,000 FDIC employees and contractors. In our evaluation report, *The FDIC's Physical Security Risk Management Process* (April 2019), we assessed whether physical security risk management processes met Federal standards and guidelines. We concluded that the FDIC had not established an effective physical security risk management process to ensure that it met ISC standards and guidelines.

We found that the FDIC frequently did not document its decisions regarding facility security risks and countermeasures, and such decisions were not guided by defined policies or procedures. Instead, FDIC officials relied on a few experienced employees to make important decisions regarding physical security risks and countermeasures at facilities. Without documentation of

---

[107] Verizon, 2018 Data Breach Investigations Report, (11th Edition).
[108] Carnegie Mellon University Software Engineering Institute, *Analytic Approaches to Detect Insider Threats*, (December 9, 2015).
[109] Carnegie Mellon University Software Engineering Institute, *Analytic Approaches to Detect Insider Threats*, (December 9, 2015).
[110] GAO, *High-Risk List: Substantial Efforts Need to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 6, 2019).
[111] GAO, *GAO Adds Government-wide Personnel Security Clearance Process to "High Risk List,"* GAO Press Release, (January 25, 2018).
[112] In 1995, President Clinton, by Executive Order 12977 (October 19, 1995), created the Interagency Security Committee (ISC) in order to issue standards, policies, and best practices to enhance the quality and effectiveness of security in non-military Federal facilities in the United States.
[113] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 6, 2019).

these decisions, FDIC executives and oversight bodies were unable to fully consider and review the decisions.

We also found that the FDIC did not conduct key activities in a timely or thorough manner for determining facility risk level, assessing security protections in the form of countermeasures, mitigating and accepting risk, and measuring program effectiveness. For example, for one of its medium-risk facilities, the FDIC began, but did not complete, an assessment more than 2½ years after the FDIC occupied the leased space. Collectively, these weaknesses limited the FDIC's assurance that it met Federal standards for physical security over its facilities. We made nine recommendations to address the weaknesses in the FDIC's physical security risk management process, and five remained unimplemented at the time of this report.

Securing Sensitive and Personally Identifiable Information

During 2016, the FDIC reported a series of breaches to Congress as departing employees improperly downloaded sensitive PII, including SSNs, to removable media devices shortly before leaving the FDIC. Collectively, these breaches potentially affected over 121,000 individuals. We reported on the FDIC's handling of these breaches and its associated controls in four prior reports.[114] In our audit report, *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (September 2017), we found that the FDIC had processes to evaluate the harm to individuals affected by a breach, but the FDIC did not adequately implement those processes. For example, it took the FDIC more than 9 months to notify individuals affected by a breach. Further, in our *OIG Special Inquiry*[115] (April 2018) report we noted systemic weaknesses that hindered the FDIC's ability to respond to multiple information security incidents and breaches efficiently and effectively. The FDIC addressed the 20 recommendations we made in these two reports.

In our audit report, *The FDIC's Privacy Program* (December 2019), we assessed the effectiveness of the FDIC's Privacy Program and practices by determining whether the FDIC complied with selected provisions in privacy-related statutes and OMB policy and guidance.[116] The FDIC's Privacy Program was effective in certain areas. Specifically, the FDIC had implemented a privacy awareness and training program; identified its privacy staffing and budgetary needs; established privacy competency requirements for key staff; and took steps to ensure contractor compliance with privacy programs. However, we found that the FDIC's controls and practices for its Privacy Program in four areas assessed were either partially effective or not effective, because they did not comply with all relevant privacy laws and/or OMB policy and guidance. Specifically, the FDIC did not:

---

[114] *See* OIG Reports, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (FDIC OIG AUD-16-004) (July 2016, revised February 2017); *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (FDIC OIG AUD-17-006) (September 2017); *Controls over Separating Personnel's Access to Sensitive Information* (FDIC OIG EVAL-17-007) (September 2017); and *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (FDIC OIG-18-001) (April 2018).

[115] *OIG Special Inquiry Report, The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (April 2018).

[116] Privacy Act of 1974, 5 U.S.C. § 552a; Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. § 3501 note); Section 522 of the Consolidated Appropriations Act of 2005, Pub. L. No. 108-447, 118 Stat. 2809, amended by Consolidated Appropriations Act of 2008, Pub. L. No. 110-161, 121 Stat. 1844 (codified as amended at 42 U.S.C. § 2000ee-2); *Designation of Senior Agency Officials for Privacy* (OMB Memorandum M-05-08) (February 11, 2005); OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).

- Fully integrate privacy considerations into its risk management framework designed to categorize information systems, establish system privacy plans, and select and continuously monitor system privacy controls;
- Adequately define the responsibilities of the Deputy Chief Privacy Officer or implement Records and Information Management Unit responsibilities for supporting the Privacy Program;
- Effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII within established timeframes; and
- Ensure that Privacy Impact Assessments[117] were always completed, monitored, published, and retired in a timely manner.

Weaknesses in the FDIC's Privacy Program increased the risk of PII loss, theft, and unauthorized access or disclosure, which could lead to identity theft or other forms of consumer fraud against individuals. In addition, weaknesses related to the management of Privacy Impact Assessments reduced transparency regarding the FDIC's practices for handling and protecting PII. Our report contained 14 recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and practices.

In addition, in our audit report, *The FDIC's Information Security Program – 2019* (October 2019), we noted that the FDIC did not adequately control access to sensitive information and PII stored on its internal network and in hard copy. For example, we identified instances in which sensitive information stored on internal network shared drives was not restricted to authorized users. We also conducted unannounced walkthroughs of selected FDIC facilities and identified significant quantities of sensitive hard copy information stored in unlocked filing cabinets and boxes in building hallways.

The majority of unsecured sensitive information we found was stored in unlocked filing cabinets and boxes in building hallways. Examples included:

- Confidential bank examination information, such as Reports of Examination;
- Suspicious Activity Reports;
- Sensitive PII, such as reports containing names, SSNs, and dates of birth;
- Legal documents, analyses, and correspondence pertaining to investigations, litigation, claims, and settlements;
- Portable storage media, including a computer hard drive and CDs/DVDs (one of which was marked confidential); and
- Contracting and procurement sensitive information.

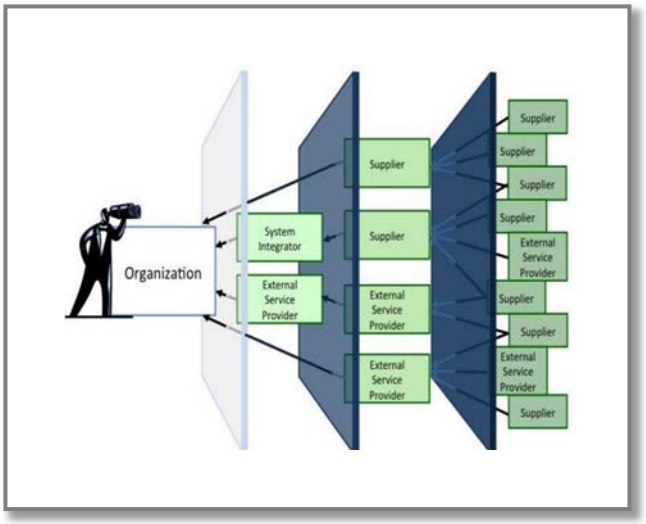
We recommended that employees and contractor personnel properly safeguard sensitive electronic and hardcopy information. The FDIC took immediate action to secure information identified by the OIG.

[117] The E-Government Act of 2002 requires, among other things, that Federal agencies conduct Privacy Impact Assessments that analyze how personal information is collected, stored, shared, and managed in a Federal system. See Government Accountability Office, *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape*, GAO-12-961T, (July 31, 2012).

Securing the FDIC's Supply Chain

According to the GAO, the supply chain is "the set of organizations, people, activities, and resources that create and move a product from suppliers to end users."[118] As shown in Figure 4, an organization may have reduced visibility, understanding, and control of relationships with vendors who rely on second- and third-tier suppliers and service providers. Risks are realized when the supply chain exploits existing vulnerabilities though it may take years for such exploitation to occur or for an agency to discover the exploitation.[119]

Figure 4: Supply Chain Risk View



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

The GAO noted that key supply chain threats include:

- **Installation of hardware or software containing malicious logic** causing significant damage by allowing attackers to take control of entire systems and read, modify, or delete sensitive information, disrupt operations, launch attacks against other organizations' systems, or destroy systems.
- **Installation of counterfeit hardware or software** threatening the integrity, trustworthiness, and reliability of information systems because they fail more often and more quickly, and provide an opportunity to insert a back door to give an intruder remote access.
- **Failure or disruption in the production or distribution of critical products**, including manmade and natural disruptions of the supply of IT products critical to federal agencies.
- **Reliance on a malicious or unqualified service provider** who can use its access to systems and data to gain access to information, commit fraud, disrupt operations, or launch attacks against other computers or networks.
- **Installation of hardware or software that contains unintentional vulnerabilities** such that defects in code or misconfigurations can be exploited to gain access to information systems and data and disrupt service.[120]

An example of supply chain risk is the Federal Government's limitation on the purchase of telecommunications equipment from Huawei because of concern that the Chinese government can access phone calls and information.[121]

The FDIC does not have a comprehensive, FDIC-wide supply chain risk policy. The FDIC's Chief Information Officer Organization (CIOO) established a *Policy on Supply Chain Risk Management* in July 2019 that applies to CIOO employees who "participate, support, and are involved with the procurement and acquisition process of IT products." Other FDIC Divisions and Offices are not bound by and may not be aware of the CIOO Policy. The FDIC established a Supply Chain Risk Management Steering Committee in 2019 to address this area of risk. We have work planned to assess the FDIC's supply chain risk mitigation.

[118] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T, (July 12, 2018).
[119] National Institute of Standards and Technology (NIST) Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.
[120] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T, (July 12, 2018).
[121] The New York Times, *U.S. Moves to Ban Huawei From Government Contracts*, (August 7, 2019).

Sustaining a Work Environment Free from Discrimination, Harassment, and Retaliation

Federal facilities should also have working environments that are free from intimidating, hostile, or offensive behaviors. Employee behaviors such as sexual harassment can undermine an agency's mission by creating a hostile work environment that lowers productivity and morale, affects the agency's authority and credibility, and exposes the agency to litigation risk and costs.

The FDIC reported receiving a total of just 9 allegations of sexual harassment over a 3½-year period (January 2015 to June 2018). However, when the Merit Systems Protection Board (MSPB) conducted a survey in 2016 (based on data from 2014 to 2016), the MSPB found that approximately 9 percent of the 427 FDIC employees who responded to the survey (40 employees) indicated they had experienced sexual harassment. We have ongoing work to review the FDIC's program for addressing sexual harassment allegations.

Conducting Background Investigations

During late 2015 and early 2016, the FDIC experienced eight 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 plans submitted by certain large systemically important financial institutions without authorization.

FDIC employees and contractors are subject to background investigations commensurate with the sensitivity of their positions, scope of responsibility, and access to classified National Security Information.[122] The FDIC's Personnel Security and Suitability Program (PSSP) aims to ensure that FDIC employees and contractors have suitable character, reputation, honesty, integrity, and trustworthiness. A strong PSSP reduces the risk of employee or contractor information breaches and identifies potential issues for the FDIC's Insider Threat Program.[123]

The FDIC does not have a policy to ensure proper coordination and collaboration among its PSSP and its Insider Threat Program. As a result, program interconnections are made at the discretion of program personnel. Absent standard criteria for the referral of potential insider threat issues from the PSSP to the Insider Threat Program Manager, threat information may not be shared. We have an evaluation underway to assess the current state of the FDIC's Personnel Security and Suitability Program.

The protection of employees, contractors, facilities, and information is paramount for the execution of the FDIC's mission and the protection of the privacy of FDIC personnel and contractors as well as financial institution customers and employees. The FDIC should ensure that it implements appropriate controls to assess the suitability of its employees and contractors and provide them with safe facilities in which to conduct their work. FDIC employees and contractors must also be responsible in protecting sensitive information and individual privacy.

[122] FDIC Circular 1610.2, *Personnel Security Policy and Procedures for FDIC Contractors;* Circular 1600.3, *National Security Program*; and Circular 2120.1, *Personnel Suitability Program*.
[123] Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position,* (June 12, 2017).

8|ADMINISTERING THE ACQUISITION PROCESS

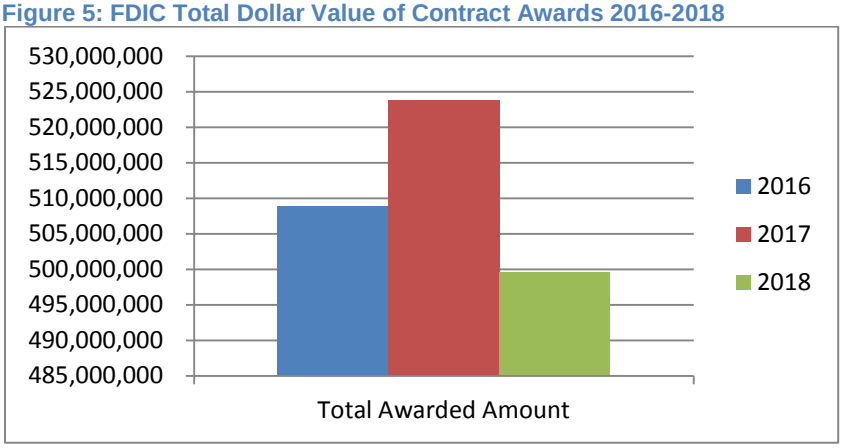
The FDIC relies on contractors for day-to-day support of its mission. In 2018, the FDIC spent nearly $500 million on contracts, with the largest expenditures for IT and administrative support services. The FDIC currently oversees acquisitions on a contract-by-contract basis—rather than on a portfolio-wide basis—and it does not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency and does not maintain certain key data elements. Therefore, FDIC officials cannot readily analyze historical contracting trends across the portfolio and identify anomalies. In addition, contracting demands are expected to increase as the FDIC modernizes its IT program and systems and moves to cloud computing. Further, FDIC contracting staff may experience significant spikes in contracting work during periods of crises. FDIC contract oversight should also include consideration of supply chain risks for acquired products and services.

According to the GAO, about 40 percent of the Government's discretionary spending is for goods and services contracts.[124] In Fiscal Year 2018, the Federal Government spent more than $550 billion on these contracts, an increase of more than $100 billion from 2015. The Administration found that major government acquisitions often failed to achieve their goals because of project management skill shortcomings among Federal procurement staff.[125] Similarly, the GAO found that Federal agencies continue to award management support service contracts but raised questions about agencies' capacity to manage those contracts.[126] Specifically, the GAO identified three challenges aligned with the contracting life cycle: (1) requirements definition, (2) competition and pricing, and (3) contractor oversight. The GAO noted that heavy workloads of contract officials at one agency made it difficult for them to oversee contracts and ensure contractors' adherence to contract terms.[127]

The FDIC procures goods and services to augment its internal resources and help the Agency achieve its mission. FDIC contracting requirements increase significantly during times of crises to address the FDIC's receivership responsibilities. The FDIC DOA Acquisition Services Branch (ASB) works with Oversight Managers (OMs) from FDIC Divisions and Offices to provide oversight of FDIC procurements. As shown in Figure 5, ASB awarded more than 2,400 contracts valued at over $1.5 billion over a 3-year period from 2016 to 2018. The average annual awarded amount per contract for these 3 years was more than $675,000.

[124] GAO WatchBlog, Federal Government Contracting for Fiscal Year 2018 (infographic) posted May 28, 2019. GAO launched its WatchBlog in January 2014, as part of its continuing effort to reach its audiences—Congress and the American people—where they are currently looking for information.
[125] President's Management Agenda, (March 20, 2018).
[126] GAO, *Federal Acquisitions: Congress and the Executive Branch Have Taken Steps to Address Key Issues, but Challenges Endure*, GAO-18-627, (September 2018).
[127] GAO, *Federal Acquisitions: Congress and the Executive Branch Have Taken Steps to Address Key Issues, but Challenges Endure*, GAO-18-627, (September 2018) (Heavy workloads were noted for the Department of Veterans Affairs.)

Figure 5: FDIC Total Dollar Value of Contract Awards 2016-2018



Source: FDIC Analysis of FDIC Contract Awards.

In 2018, the FDIC's DIT, DOA, and DRR accounted for over 96 percent of contracts and contracting dollar awards. The Chief Information Officer Organization identified specific acquisition strategies to sustain legacy systems, modernize information technology, and adapt to change. DIT expects to increase contracting activity as it implements the FDIC's *IT Modernization Plan*.

Strengthening FDIC Contract Oversight

Our evaluation report, *Contract Oversight Management* (October 2019), concluded that the FDIC must strengthen its contract oversight management. We found that the FDIC needed to improve its contracting management information system, contract documentation, the training and certification of certain OMs, and workload capacity of OMs for one Division.

Specifically, we found that the FDIC was overseeing acquisitions on a contract-by-contract basis rather than on a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. For example, the FDIC's contracting system did not maintain certain key data in a manner necessary to conduct historical trend analyses, plan for future acquisition decisions, and assess risk in the FDIC's awarded contract portfolio. As a result, FDIC Board Members and other senior management officials were not provided with a portfolio-wide view or the ability to analyze historical contracting trends across the portfolio, identify anomalies, and perform ad hoc analyses to identify risk or plan for future acquisitions.

Additionally, 20 percent of the contracts executed between 2013 and 2017 (1,518 of 7,786) did not have contract pricing arrangement information entered into the FDIC's Automated Procurement System. Without complete data, the FDIC cannot readily analyze the contract pricing arrangements across the FDIC's contract portfolio.

We also found that contract files maintained by OMs were often incomplete, and that OMs were unable to produce the missing contract documentation, such as critical records relating to inspection and acceptance. Without this documentation, the FDIC could incur additional costs to recover or replace lost documentation and could have difficulty enforcing the contract in the event of contractor noncompliance.

Further, OMs improperly uploaded contractor deliverable documentation containing PII to the FDIC's contacting system known as CEFile for one of our four sampled contracts covering

property management services for failed bank properties. Because CEFile was not identified as a system to retain PII, the FDIC was not monitoring CEFile for PII. Therefore, there was a risk that the PII in CEFile could be improperly accessed, printed, and removed. The FDIC subsequently took action to remove the PII from CEFile.

We also found that the workload for OMs in DIT was 67-percent higher than another FDIC Division with a similar-sized contract portfolio. DIT acknowledged that insufficient OM capacity put it at risk for ineffective oversight. We made 12 recommendations in the *Contract Oversight Management* report.

In two previous OIG evaluation reports, we identified similar issues involving DIT oversight.

- In *Payments to Pragmatics, Inc*. (December 2018), we determined that about 10 percent 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.

- In the *FDIC's Failed Bank Data Services Project* (March 2017), we reviewed transition costs ($24.4 million) of a 10-year project to replace the FDIC's information systems for processing bank data for failed financial institutions. We found that the FDIC faced challenges related to defining contract requirements, coordinating contracting and program office personnel, and establishing 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.

Reviewing for Supply Chain Risk

When an agency contracts for goods and services that will be introduced into its environment, the agency might encounter risks related to product and service supply chains. Management of supply chain risk requires "ensuring the integrity, security, quality, and resilience of the supply chain and its products and services."[128]

Supply chain risk is not limited to equipment. Contractor personnel also pose security risks to organizations, especially contractors involved in systems development. Contractors with malicious intent may be able to insert harmful hardware or malicious code into FDIC systems.

NIST advises organizations to take a holistic, enterprise-wide approach to managing supply chain risks.[129] Organizational best practices include executive-level involvement in supply chain risk management decision-making and cross-functional leadership structures to break down silos. In addition, as required by statute, OMB has initiated a Federal Acquisition Security

[128] NIST, Cyber Supply Chain Risk Management, (May 24, 2016).
[129] NIST Special Publication 800-161, *Supply Chain Risk Management for Federal Information Systems and Organizations*, (April 2015).

Council to assist Federal agencies in determining supply chain risk, sharing supply chain risk information, and deciding on actions to mitigate risk.[130]

As mentioned previously, the FDIC does not have a comprehensive, FDIC-wide supply chain risk policy. The FDIC's CIOO has a supply chain risk policy applicable to CIOO IT procurements. Thus, FDIC personnel outside the CIOO are not currently required to consider or mitigate supply chain risks as part of procurement activities.

Further, the responsibility of managing FDIC supply chain risk is not within the FDIC's contracting staff but is a collateral duty for the FDIC's Insider Threat Program Manager. As a result, supply chain risk management is not the focus of those involved in the contracting process. The FDIC established a Supply Chain Risk Management Steering Committee in 2019 to address this area of risk. We will be monitoring and assessing the FDIC's efforts in this regard.

Contracting is an important function at the FDIC because of the Agency's reliance on outsourced services, especially during times of crises. In order to establish an effective contracting oversight program, the FDIC should maintain a contracting system that can readily provide an adequate portfolio-wide view of the Agency's acquisitions. In addition, the FDIC should establish an effective program to manage and mitigate supply chain risks.

9|MEASURING COSTS AND BENEFITS OF FDIC REGULATIONS

Financial regulations significantly affect banks and their customers. The FDIC does not currently have a consistent process in place to determine when and how to conduct cost benefit analysis in order to ensure that the benefits of a regulation justify its costs. Further, the FDIC does not have criteria in place to distinguish among rules which are sufficiently "significant" to require cost benefit analysis. Absent clear processes and criteria, demonstrating that FDIC regulations justify their costs remains a fundamental challenge. We also note that the FDIC does not conduct retrospective cost benefit analyses on existing rules. Performing such analyses would help the FDIC ensure that its rules are effective and achieve their intended objectives/outcomes.

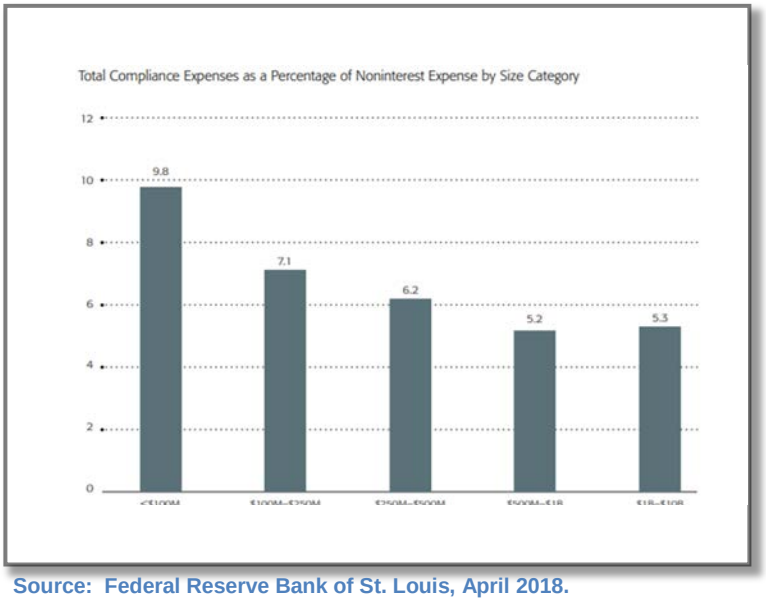
According to a study by the Federal Reserve Bank of St. Louis, regulatory compliance costs as a percentage of overall non-interest expense for small banks are nearly twice those of larger banks.[131] As shown in Figure 6, for the years of 2015 through 2017, small banks (less than $100 million in assets) incurred total compliance costs at 9.8 percent of their noninterest expenses. By comparison, banks with $1 to $10 billion in assets had compliance costs at 5.3 percent of their noninterest expenses for the same period.

[130] Director of National Intelligence, *Supply Chain Risk Management*, National Supply Chain Integrity Month, (April 24, 2019). See also The Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018, Public Law No. 115-390 (December 21, 2018) ("SECURE Technology Act"). Title II of the Act established the Federal Acquisition Security Council (FASC).

[131] Federal Reserve Bank of St. Louis, *Compliance Costs, Economies of Scale and Compliance Performance, Evidence from a Survey of Community Banks,* (April 2018).

In August 2018, the FDIC Chairman stated that a top priority for the Agency was to review the regulatory burden on small banks.[132] She further emphasized the need to balance regulatory safety and soundness requirements without impeding banks' ability to compete. The challenge, she indicated, is to ensure that FDIC regulations are appropriate to the size and complexity of the banks that the FDIC supervises.[133]

Figure 6: Total Compliance Expenses as a Percentage of Noninterest Expenses



Source: Federal Reserve Bank of St. Louis, April 2018.

Quantifying Costs and Benefits

According to the *FDIC's Statement of Policy on the Development and Review of Regulations and Policies*, the FDIC uses available information to evaluate the costs and benefits of reasonable and potential regulations or statements of policy. Quantifying both the costs and benefits of significant financial regulations is challenging, and it often may be imprecise and unreliable.[134] Performing such analysis can be difficult, because it involves theory, modeling, statistical analysis, and other tools to predict future outcomes based on certain assumptions.[135] For example, it may be difficult to estimate the cost of a financial crisis and the benefits of regulations aimed to eliminate the crisis.[136] Congress acknowledged the difficulty in measuring costs and benefits when introducing the Independent Agency Regulatory Analysis Act (March 25, 2019). This Act requires agencies to "assess the costs and benefits of the intended rule and, recognizing that some costs and benefits are difficult to quantify, propose or adopt a rule only upon a reasoned determination that the benefits of the rule justify the costs."[137]

In our evaluation report, *Cost Benefit Analysis Process for Rulemaking* (February 2020), we evaluated whether the FDIC's cost benefit analysis process for rules was consistent with best practices. We found that the FDIC's cost benefit analysis was not consistent with best practices, because the FDIC did not:

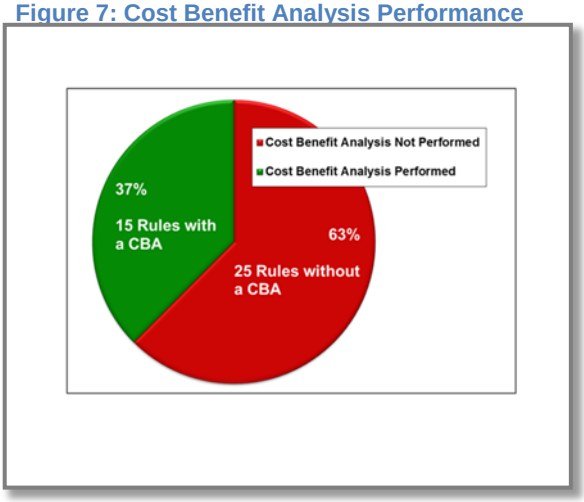
- Establish and document a process to determine when and how to perform a cost benefit analysis;
- Leverage the expertise of its economists when rules were initially developed;
- Require the FDIC Chief Economist to concur on the cost benefit analyses performed;
- Disclose its cost benefit analyses to the public; and
- Perform cost benefit analyses after final rule issuance.

---

[132] Wall Street Journal, *New FDIC Leader Joins Push to Re-Evaluate Banking Rulebook*, (August 6, 2018).
[133] Jelena McWilliams, FDIC Chairman, *"Principles of Supervision,"* delivered at the American Bar Association Banking Law Committee Annual Meeting (January 11, 2019).
[134] Yale Law Review, *Cost-Benefit Analysis of Financial Regulation: A Reply*, (January 22, 2015).
[135] Congressional Research Service, *Cost-Benefit Analysis and Financial Regulator Rulemaking*, (April 12, 2017).
[136] The University of Chicago Journal of Legal Studies, *Challenges for Cost-Benefit Analysis of Financial Regulation*, (June 2014).
[137] *Independent Agency Regulatory Analysis Act, S. 869*, United States Senate, (March 26, 2019).

The FDIC's rulemaking process resulted in inconsistent practices for conducting cost benefit analyses. As shown in Figure 7, based on our review of rules promulgated by the FDIC from January 2016 to December 2018, we found that the FDIC performed cost benefit analyses on 37 percent of the final rules published in the Federal Register. The FDIC did not explain in the accompanying Federal Register notices why 15 rules needed a cost benefit analysis and the other 25 rules did not. These rules lacking a cost benefit analysis included both substantive rules and technical modifications.

Figure 7: Cost Benefit Analysis Performance



Source: OIG analysis of FDIC rules published in the Federal register.

The FDIC also did not have an established process for determining how to perform cost benefit analyses. Based on our review, we found that the FDIC performed an in-depth cost benefit analysis[138] on only 10 percent of the final rules published in the Federal Register.

In addition, the depth of analysis that the FDIC performed did not always align with the rule's degree of significance.[139] We found substantive rules without corresponding cost benefit analyses, and less substantive rules with cost benefit analyses. The process used by the FDIC did not ensure that the Agency identified and defined a proposed rule's degree of significance, and that the Agency appropriately and consistently analyzed costs and benefits.

We also noted that the FDIC did not conduct retrospective cost benefit analyses on existing rules.[140] Without performing cost benefit analyses of existing rules, the FDIC may not identify duplicative, outdated, or overly burdensome rules in a timely manner. In addition, the FDIC may not ensure that its rules are effective and achieve their intended objectives/outcomes. We made five recommendations to the FDIC to improve the cost benefit analysis in its rulemaking process.

---

[138] The OIG defines an "in-depth" cost benefit analysis as a cost benefit analysis that contains supporting quantitative and qualitative data and analysis of the proposed action and main alternatives identified.

[139] Executive Order 12866 advises Federal agencies, not including the FDIC, to conduct in-depth cost benefit analyses for certain significant regulatory actions. The order defines significant regulatory action as any regulatory action that is likely to result in a rule that may: (1) have an annual effect on the economy of $100 million or more, or adversely affect in a material way the economy, or a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this order.

[140] Under the Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA) (12 U.S.C. § 3311 (1996)), the FFIEC and certain member agencies (Federal bank regulators – FDIC, OCC, and FRB), and the NCUA (as a participating member), are directed to conduct a joint review of their regulations every 10 years and to consider whether any of those regulations are outdated, unnecessary, or unduly burdensome. Since Congress enacted EGRPRA in 1996, the FDIC (jointly with other agencies under the FFIEC) has completed two reviews and submitted two reports to Congress – the first report was submitted in 2007 and the second report was submitted in 2017. The FDIC performed these reviews over a period of several years, and commenced the second EGRPRA review in 2014. The FDIC's EGRPRA review process was a reactive review process that relied solely on public comments to identify and initiate Agency action on rules that may be outdated, unnecessary, or unduly burdensome.

On December 3, 2019, the FDIC issued a Request for Information seeking comment on approaches to analyzing the effects of its regulatory actions and alternatives. In addition, on November 4, 2019, the FDIC announced a reorganization that moved the regulatory analysis function from the Office of the Chief Economist to the Research and Regulatory Analysis Branch, which also houses the FDIC's Center for Financial Research. We will continue to monitor this realignment.

The FDIC should accurately measure costs and benefits to ensure that regulations strike the proper balance between the safety and soundness at institutions and regulatory burden. Also, the FDIC should have transparent processes in place to obtain and assess reliable information to measure the impact of regulatory action. Absent such processes, FDIC rules may impose burdensome costs on banks and consumers.

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.