Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

Included in the Federal Deposit Insurance Corporation 2017 Annual Report

February 2018

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation
Office of Inspector General

Date: February 15, 2018

Memorandum To: Board of Directors

From: Jay N. Lerner
Inspector General

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

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

The FDIC's mission 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 $7.1 trillion in deposits at more than 5,700 financial institutions, and directly supervises about 3,700 of these banks. The FDIC also oversees the resolution and receivership of failed banks, consumer financial protection, and management of the Deposit Insurance Fund. Therefore, it is important to address these complex Challenges facing the agency. Moreover, the FDIC is currently at a critical juncture, particularly with respect to anticipated changes in its leadership and Board of Directors, including the position of Chairman.

This year we identified seven areas representing the most significant Challenges for the FDIC:

- Emerging Cybersecurity Risks at Insured Financial Institutions;
- Management of Information Security and Privacy Programs;
- Utilizing Threat Information to Mitigate Risk in the Banking Sector;
- Readiness for Banking Crises;
- Enterprise Risk Management Practices;
- Acquisition Management and Oversight; and
- Measuring Costs and Benefits of FDIC Regulations.

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

Attachment

TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE FEDERAL DEPOSIT INSURANCE CORPORATION

Emerging Cybersecurity Risks at Insured Financial Institutions

In August 2017, the President's National Infrastructure Advisory Council ("NIAC")[1] highlighted significant cybersecurity risks to the financial services sector and concluded that the country had "a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber attack to organize effectively and take bold action." The Federal Deposit Insurance Corporation ("FDIC"), in its Annual Performance Plan for 2017, recognized that cybersecurity was a "significant concern for the banking industry because of the industry's use of and reliance on technology, not only in bank operations, but also as an interface with customers." The FDIC Performance Plan further stated that "[c]ybersecurity has become one of the most critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber attacks."

Common Cyber-Criminal Strategies

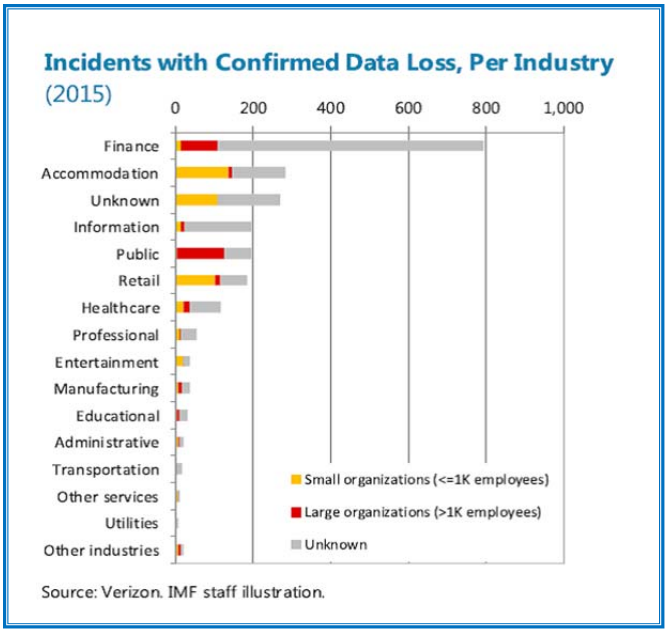
- Distributed denial-of-service – prevents customer access to bank websites and is also used as a diversionary tactic by criminals attempting to commit fraud using stolen credentials to initiate wire transfers.
- Malicious software – a broad class of attack that is generally delivered by email and lures the recipient into reading the email, opening an attachment, and providing sensitive information.
- Compound attack – deploys more than one method of attack simultaneously.
- Ransomware – limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

Sources: FDIC Supervisory Insights, *A Framework for Cybersecurity* and FFIEC Joint Statement-Cyber Attacks Involving Extortion

The Financial Stability Oversight Council ("FSOC") also underscored cybersecurity risks to the banking sector in its Annual Report (2017), stating that, "[i]f severe enough, a cybersecurity failure could have systemic implications for the financial sector and the U.S. economy more broadly."[2] The Department of the Treasury's Office of Financial Research ("OFR") Annual Report to Congress 2017 added that "[t]he financial system is an attractive target for cyber thieves and other hackers because financial companies manage the nation's wealth and handle trillions of dollars in transactions every day that underlie the U.S. economy." The International Monetary Fund Working Paper, *Cyber Risk, Market Failures, and Financial Stability* (2017), also recognized that the financial sector experienced the most cybersecurity incidents across all industries with confirmed data

[1] The NIAC was established on October 16, 2001 and advises the President, through the Secretary of Homeland Security, on security and resilience of the Nation's critical infrastructure sectors and their functional systems, physical assets, and cyber networks.

[2] The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 established the FSOC, which has accountability for identifying risks and responding to emerging threats to financial stability. The FSOC is a collaborative body that brings together the expertise of federal financial regulators (including the FDIC), an independent insurance expert appointed by the President, and state regulators. The Office of Financial Research is a bureau within the Department of the Treasury that provides support to the FSOC, the Council's member organizations, and the public.



losses in 2015, and by a substantial margin. In addition, on December 1, 2017, the Federal Reserve Vice Chair for Supervision, Randal Quarles, described cybersecurity as the biggest risk facing the financial sector and encouraged that federal banking regulators should be "bringing more of the resources of the government to bear" to boost digital defenses.[3]

The FDIC plays an important role as a financial regulator to ensure the stability of the financial system, and as the primary federal regulator of approximately 3,700 financial institutions. In addition, as of the third quarter of 2017, the FDIC provided deposit insurance coverage for 5,738 institutions with total assets of $17.2 trillion and deposits of $7.1 trillion. Therefore, the FDIC has a significant financial interest in mitigating cybersecurity risks at insured banks. If a bank fails, the FDIC will need to step in and may have to fund the losses from its Deposit Insurance Fund.

Given the significance of cybersecurity risk to U.S. financial institutions, FDIC information technology ("IT") examinations are an important tool to identify weaknesses and vulnerabilities in FDIC-supervised institutions. According to the Federal Financial Institutions Examination Council[4] ("FFIEC") *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*, "[f]inancial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly."

FDIC IT examinations assess the management of IT risks, including cybersecurity, at FDIC-supervised institutions and at select third-party technology service providers ("TSP"). When examinations identify undue risks and weak risk management practices at institutions, the FDIC may use informal or formal enforcement procedures to address those risks and practices as well as deteriorating financial conditions, or violations of laws or regulations.[5] Many financial

[3] American Banker, *Regulators Have Bigger Role to Play in Cybersecurity* (December 1, 2017).
[4] The Federal Financial Institutions Examination 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, FDIC, National Credit Union Administration, Office of the Comptroller of the Currency, and Consumer Financial Protection Bureau and to make recommendations to promote uniformity in the supervision of financial institutions.
[5] Risk Management Manual of Examination Policies, Part I 1.1 Basic Examination Concepts and Guidelines and Part IV Administrative and Enforcement Actions.

institutions maintain contracts with TSPs to outsource certain bank functions such as IT operations or business or product lines. As recognized in the Office of the Comptroller of the Currency's ("OCC") Semiannual Risk Perspectives (Spring 2017),[6] TSPs are also targets for cybercrime and may provide a back door into bank operations through the supply of IT products and services that allow remote access and management of bank operations or applications. In addition, the OCC identified concerns with large numbers of banks relying on a small number of TSPs. For example, OCC examiners identified third-party services for merchant card processing, denial of service mitigation, and trust account systems as instances of concentration among providers. As such, if a TSP has its systems or information compromised, it may significantly impact a large segment of the banking industry.

In our OIG evaluation, *Case Study of a Computer Security Incident Involving a Technology Service Provider* (2016), we reviewed allegations about a computer security incident potentially involving unauthorized access to unencrypted Personally Identifiable Information ("PII")[7] from multiple client financial institutions residing on a TSP's computer server. We concluded that a poor internal control environment and a vague incident response policy limited the TSP's ability to protect against the incident and hampered incident response efforts. The TSP did not collect or retain forensics information such as an image of the server, and it lacked a computer activity log to identify data access and exfiltration.

Further, in our OIG evaluation, *Technology Service Provider Contracts with FDIC-Supervised Institutions* (February 2017), we assessed how FDIC-supervised institutions' contracts with TSPs addressed the TSP's responsibilities related to business continuity planning and responding to and reporting on cybersecurity incidents. Based on our sample of 48 contracts with 19 institutions, we did not see evidence that most financial institutions reviewed fully considered and assessed the potential impact that TSPs may have on the institution's business continuity planning and cybersecurity incident response and reporting operations.

In 2015, we issued an OIG evaluation report, *The FDIC's Supervisory Approach to Cyberattack Risks*, which found inconsistencies in the quality and depth of IT examination assessments and documentation of findings among examiners, because examiners had discretion in conducting and documenting IT work. We also found a few situations where IT examinations of complex financial institutions were led by individuals that either did not have sufficient IT expertise or

[6] These risks were recently reiterated in the OCC's Semiannual Risk Perspective (Fall 2017) released on January 18, 2018.
[7] According to OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, the term PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

required on-the-job training. The FDIC has taken steps described in the paragraphs below to address issues identified in these reports.

In July 2015, the Government Accountability Office ("GAO") issued a report, *Cybersecurity: Banks and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*. GAO examined how the bank regulators – the FDIC, the OCC, and the Federal Reserve Board – oversee financial institutions' efforts to mitigate cyber risk. The GAO found that the regulators were not routinely aggregating and analyzing data on IT deficiencies found in individual financial institutions in order to analyze trends in specific security problems across institutions and use that information to better target future examinations.

In the last 2 years, the FDIC modified its IT examination process, in part in response to concerns identified. In July 2016, the FDIC implemented a new Information Technology Risk Examination ("InTREx") program for financial institutions. InTREx provides baseline work programs supplemented by FFIEC Information Technology Examination Handbook (IT Handbook) programs for more complex or high-risk areas. A work program provides a series of questions and steps to guide examiners. The IT Handbook also provides examination procedures for TSPs. According to the FDIC, InTREx enhances identification, assessment, and validation of IT and operations risks in financial institutions. InTREx contains both structured and unstructured information that should facilitate supervisory tasks and horizontal analysis across institutions. We will be conducting an audit that will assess the InTREx program.

A key challenge associated with IT examinations is ensuring that the FDIC has the right number of examiners with appropriate skills, training, and experience to match institution IT complexity. According to the FDIC's InTREx Program Examination Procedures, examiner staffing is based on a financial institution's Information Technology Profile ("ITP") questionnaire score. Upon receipt of the completed ITP information, the FDIC validates the profile, makes qualitative adjustments, and determines the net technology score that translates into a complexity level of high, medium, or low. The FDIC then attempts to match the examiner's IT training to the complexity of the institution's IT systems. Thus, a highly complex bank requires an examiner trained in advanced IT skills.

During 2016, the FDIC trained 1,594 field examiners in InTREx low-complexity IT examination processes and completed a reorganization that established a new Operational Risk Branch led by a Deputy Director. In addition, the FDIC advised that it had established a new IT supervision group, updated its core IT training for examiners, added an IT examination requirement for examiners, increased the pace of IT subject-matter expert training, and hired term IT specialists.

We are planning to conduct an evaluation of the FDIC's approach to examiner staffing, including IT examination resources.

In addition to examinations, the FDIC provides cybersecurity awareness resources to financial institutions. For example, the FDIC, through the FFIEC website, provides bankers with access to technical assistance videos, articles, exercises, and Financial Institution Letters ("FIL")[8] that address cybersecurity risks. According to OIG analysis, the FDIC issued 21 FILs related to cybersecurity to Chief Executive Officers at financial institutions between January 2008 and December 2017. These FILs included information such as cybersecurity awareness webinars (October 25, 2016), introduction of cybersecurity assessment tools (July 2, 2015), and statements on malware (March 30, 2015). The FFIEC also issues statements and alerts to financial institutions regarding threats and vulnerabilities. Between October 2013 and May 2017, the FFIEC issued 15 statements and alerts related to cybersecurity. To illustrate, in June 2016, the FFIEC issued a statement advising financial institutions to review risk management practices and controls over payment networks.

The FDIC must continue its efforts to mitigate cybersecurity risks at financial institutions and TSPs in order to protect the Deposit Insurance Fund and consumers. In this regard, the FDIC should continue building its capabilities to assess IT risks and trends and deploy IT examination staff commensurate with risks at FDIC-supervised institutions. Further, the FDIC should take prompt supervisory action when banks do not have effective information security programs.

[8] FILs are addressed to the Chief Executive Officers of financial institutions and are used by the FDIC to announce new regulations and policies, new FDIC publications, and a variety of other matters of principal interest to those responsible for operating a bank or savings association.

Management of Information Security and Privacy Programs

According to the United States Computer Emergency Readiness Team ("US-CERT"), from 2014 through 2016, federal government agencies reported more than 177,000 cybersecurity incidents, with more than 50,000 involving PII.[9] GAO's report, *High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* (2017), recognized that safeguarding computer systems from cyber threats is a high risk across the Federal government and has been a long-standing concern for over 20 years. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.

In 2015, the records of the Office of Personnel Management were compromised. The computer hack resulted in the theft of records containing the PII of more than 21 million prospective, current, and former Federal employees. This breach alone is estimated to cost $350 million for credit and identity monitoring services, identity theft protection, and identity restoration services for affected individuals. This data breach brought into focus the need for strong management of information security and privacy protection programs within the FDIC.

Recent guidance from the Office of Management and Budget ("OMB"), OMB Memorandum M-17-12, entitled *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), further describes the gravity of cybersecurity breaches: "Identity theft represented 16 percent (490,220) of the over 3 million complaints received by the Federal Trade Commission ("FTC") in 2015. In 2014, the Department of Justice reported that 17.6 million individuals or 7 percent of all U.S. residents age 16 or older, were victims of one or more occurrences of identity theft."

The FDIC uses IT systems and applications to perform its several mission goals regarding safety and soundness for financial institutions, consumer protection, managing the Deposit Insurance Fund, and resolution and receivership of failed institutions. These systems and applications hold significant amounts of sensitive data.[10] For example, the FDIC's Failed Bank Data System contains more than 2,500 terabytes of sensitive information from more than 500 bank failures.

---

[9] US-CERT is an organization within the Department of Homeland Security that assists federal civilian agencies with their data breach incident handling efforts. The Federal Information Security Modernization Act of 2014 ("FISMA 2014") requires federal agencies to report security incidents to US-CERT, which analyzes the information to identify trends and indicators of attack across the federal government.

[10] FDIC Circular 1360.9, *Protecting Sensitive Information*, defines sensitive information as "information that contains an element of confidentiality. It includes information that is exempt from disclosure by the Freedom of Information Act and information whose disclosure is governed by the Privacy Act of 1974. Sensitive information requires a high level of protection from loss, misuse, and unauthorized access or modification."

In addition, FDIC systems contain substantial amounts of PII, including, for example, names, Social Security Numbers, and addresses related to bank officials, depositors, and borrowers at FDIC-insured institutions and failed banks, and FDIC employees. Of the FDIC's 261 system applications, 151 applications required Privacy Impact Assessments because they collect, maintain, or disseminate PII.

Over time, the FDIC has experienced a number of cybersecurity incidents. In August 2011, the FDIC began to experience a sophisticated, targeted attack on its network known as an Advanced Persistent Threat ("APT").[11] The attacker behind the APT penetrated more than 90 workstations or servers within the FDIC's network over a significant period of time, including computers used by the former Chairman and other senior FDIC officials. The attacker further gained unauthorized access to a significant quantity of sensitive data. The FDIC's Division of Information Technology failed to fully inform senior FDIC executives of the severity and magnitude of the intrusion. In response to this incident, the FDIC hired a cybersecurity firm to perform additional analysis and realigned its IT functions.

In late 2015 and early 2016, the FDIC was again impacted by significant cybersecurity incidents. In this case, the FDIC detected eight data breaches as departing employees improperly took sensitive information shortly before leaving the FDIC. The FDIC initially estimated that this sensitive information included the PII of approximately 200,000 individual bank customers associated with approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions; however, the FDIC later revised the number of affected individuals to 121,633.

In our OIG report, *The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans* (July 2016), we reviewed the September 2015 breach in which a former employee copied, without authorization, highly confidential components of three sensitive resolution plans onto an unencrypted Universal Serial Bus ("USB") storage device and took the information upon abruptly resigning. OIG law enforcement officials subsequently recovered the USB device containing all of the exfiltrated data as well as a sensitive Executive Summary for a fourth resolution plan in hard copy. Based on the OIG criminal investigation, the employee was subsequently charged in the Federal District Court for the Eastern District of New York with theft of government property (18 U.S.C. Section 641).

In another OIG report, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (July 2016), we reviewed the FDIC's process to address the breach involving

[11] An advanced persistent threat may occur when an entity gains unauthorized access to a computer network, escalates its privileges, and develops an ongoing presence within the network to compromise the network data and component-level security.

an employee's use of a USB storage device to copy more than 10,000 documents, including more than 10,000 unique Social Security Numbers upon the employee's departure from the FDIC. We found that over 4 weeks elapsed between the discovery of the incident and a determination that the incident involved a data breach. We concluded the FDIC had not devoted sufficient resources to review potential violations.

In a recent OIG report, *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (September 2017), we assessed the adequacy of the FDIC's processes to evaluate the risk of harm to individuals affected by a breach of PII and to notify and provide services to those individuals when appropriate. We reviewed a sample of suspected or confirmed breaches occurring between January 1, 2015 and December 1, 2016, potentially affecting 13,000 individuals. We found that the FDIC did not notify affected individuals until more than 9 months had elapsed from the date of discovery of the breaches. Further, we noted that the FDIC had not devoted sufficient resources to address a dramatic increase in breach investigation activities. We also determined that the individuals responsible for examining the data breaches did not always have the necessary skills and training to ensure proper performance of their duties.

In another recent OIG report, *Audit of the FDIC's Information Security Program – 2017* (October 2017), we identified FDIC security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. Security control weaknesses included, for example:

- **Contingency Planning.** The FDIC's IT restoration capabilities were limited, and the agency had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster.
- **Information Security Risk Management.** The FDIC established the Information Security Risk Advisory Council ("the Council") in 2015. However, the Council did not fulfill several of its key responsibilities as defined in FDIC policy.
- **Enterprise Security Architecture.** The FDIC had not established an enterprise security architecture that (i) describes the FDIC's current and desired state of security and (ii) defines a plan for transitioning between the two. The lack of an enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain.
- **Technology Obsolescence.** The FDIC was using certain software in its server operating environment that was at the end of its useful life and for which the vendor was not providing support to the FDIC.
- **Information Security Strategic Plan.** The FDIC had drafted, but not yet finalized, an information security strategic plan.

- **Patch Management.** We noted instances in which patches addressing high-risk vulnerabilities were not installed on servers, desktop computers, and laptop computers within the timeframes established by FDIC policy.
- **Credentialed Scanning.** We found instances in which network IT devices were not subject to a "credentialed" scan—a thorough type of scan that involves logging into the IT device to inspect for vulnerabilities.
- **Security Information and Event Management ("SIEM") Tool.** The FDIC had not developed a process to ensure that all servers on the FDIC's network routed log data to the FDIC's SIEM tool.

We determined that, according to the FISMA Reporting Metrics, the FDIC was rated as "Defined," which indicated that policies and procedures were formalized and documented, but not consistently implemented.

GAO also assessed information security controls over key financial systems, data, and networks as part of its audit of the FDIC's financial statements. In its report, *Information Security: FDIC Needs to Improve Controls over Financial Systems and Information* (May 2017), GAO identified information security deficiencies at the FDIC. For example, GAO found that the FDIC did not implement sufficient controls to isolate financial systems from other parts of its network to prevent unauthorized users and systems from communicating with the financial systems. Further, GAO reported that the FDIC did not implement sufficient controls over a privileged account used by systems engineers to manage the FDIC's virtual environment. As a result, the FDIC had diminished ability to distinguish between authorized and unauthorized activity in the systems. According to GAO, those information system control issues "represented a significant deficiency in the FDIC's internal control over financial reporting systems as of December 31, 2016."[12]

Weaknesses in Management of Contractor Personnel. Our OIG report, *Controls over Separating Personnel's Access to Sensitive Information* (September 2017), identified weaknesses in the management of contractor access to FDIC systems, data, and facilities. We found that separating contractor employees may present greater risks than FDIC employees, because the FDIC may not know as much about an individual contractor's personnel history and the contractor may depart without advanced notice. Further, we found that the priority review of network activity using the Data Loss Prevention ("DLP")[13] tool was not conducted in the pre-exit clearance process for many contractors. We estimated that at least 43 percent of FDIC

[12] At the time of issuance of this report, we were advised by the FDIC that the GAO had not identified a significant deficiency in the FDIC's internal control over financial reporting as of December 31, 2017.

[13] The DLP operates as a guard around the digital perimeter of the FDIC and monitors various electronic ways sensitive information could leave the FDIC. For example, the DLP monitors outgoing emails, documents sent to network printers, website uploads, and downloads to external media.

contractors who separated between October 1, 2015 and September 30, 2016 were not subject to such DLP priority review. In addition, the FDIC could not locate clearance records for 46 percent of the contractors we sampled, and records management liaisons did not review data questionnaires before contractors separated in 94 percent of the cases we reviewed.

Further our OIG report, *Follow-on Audit of the FDIC's Identity, Credential, and Access Management Program* (June 2017), found that the FDIC did not maintain current, accurate, and complete contractor personnel data to ensure Personal Identity Verification ("PIV") card (*i.e.*, a badge) credential issuance to authorized FDIC contractors. Absent reliable contractor information, PIV cards may not be issued and revoked in a timely manner, presenting an increased risk of unauthorized access to FDIC facilities and networks.

Contracts for IT goods and services also pose risks because there are often multiple tiers of outsourcing, as well as numerous actors such as suppliers, acquirers, systems integrators, and service providers that interact to design, manufacture, and deploy products and services. The National Institute of Standards and Technology described the vulnerabilities in the "supply chain" for U.S. Government agencies to include the influence of foreign governments, counterfeit products, unauthorized production, tampering, and insertion of malicious software and hardware. For example, on December 12, 2017, legislation was enacted that banned the U.S. Government's use of Kaspersky Labs, a supplier of antivirus products, due to concerns of foreign government influence. The FDIC contracts for the purchase of laptops, servers, and other IT products in support of its mission and should maintain awareness of supply chain risks.

Change in Cyber Management at FDIC. Turnover in key leadership positions affected the management of the FDIC's cybersecurity and privacy programs. Between 2010 and 2017, the FDIC had seven acting or permanent Chief Information Officers ("CIO") who also held the role of Chief Privacy Officer ("CPO"). During this same period of time, the FDIC also had seven Chief Information Security Officers. These senior management changes impact the direction of an organization because turnover affects management strategy, planning, budgets, and staffing. As noted by GAO in *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges* (2004), a high turnover rate in CIOs negatively impacts their effectiveness because there is limited time to put their agenda in place or form close working relationships with agency leadership. In the case of the FDIC, the turnover hindered progress in establishing and implementing an IT governance framework, such as an Enterprise Architecture, IT Strategic Plan, and Information Security Plan—all of which are fundamental to a successful IT program.

A recent example highlights how turnover experienced by the FDIC contributed to the underlying challenge of managing information security. The former CIO at the FDIC

(November 2015 to October 2017) began an initiative to move FDIC IT operations to cloud-based solutions. Adopting a cloud-based IT approach reflected a significant change not contemplated in the governance documents referenced above, as it moved IT procurement, development, and maintenance from on-site services to off-site services. Such a move involved migrating the FDIC's data center to a contractor owned and operated facility and a shift in FDIC IT personnel skills, governance, and policies and procedures towards oversight, management, and monitoring of cloud contracts. However, the FDIC's current CIO decided to take a more measured approach by moving some IT operations to the cloud in October 2017. FDIC resources devoted to cloud strategy planning from March to October 2017 could have been deployed to other IT initiatives.

The FDIC's Privacy Program. The FDIC has designated its CIO as the CPO, also referred to as the Senior Agency Official for Privacy ("SAOP"). Notably, however, OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, states that "agencies should recognize that privacy and security are independent and separate disciplines. While privacy and security require coordination, they often raise distinct concerns and require different expertise and different approaches. The distinction between privacy and security is one of the reasons that the Executive Branch has established a Federal Privacy Council independent from the Chief Information Officers Council."

In light of the updated requirements and responsibilities for the SAOP/CPO, the FDIC may wish to consider whether the CIO should continue to serve as SAOP/CPO. The perspectives of the SAOP/CPO are different from those of the CIO. The CIO has responsibility for maintaining a broad, strategic orientation focused on enterprise issues and concerns and protecting the agency's IT resources. These issues relate to the management of the FDIC's IT systems, enterprise architecture, governance of programs and resources, acquisition of hardware, backup systems, personnel, security systems, and processes to keep the IT systems running efficiently and effectively. In contrast, the CPO's (and SAOP's) role is oriented towards protecting the privacy of individuals, including FDIC programs, policies, and procedures that affect bank customers and FDIC personnel, and reducing the risk of harm to potentially affected individuals in the event of a breach.

Also, the SAOP/CPO has responsibility for privacy issues and concerns that extend beyond IT issues. For example, the SAOP/CPO has responsibilities for privacy implications related to FDIC materials that are not in electronic form. In addition, the SAOP/CPO is responsible for the privacy implications of internal FDIC programs that might affect FDIC personnel. The SAOP/CPO is further responsible for the privacy implications of disclosures of information outside of the FDIC, and this official may need to make decisions about the laws and regulations governing

privacy law, discovery productions in litigation, Freedom of Information Act requests, and other disclosure laws and regulations.

The FDIC's Performance Plan for 2017 indicated that it would prioritize efforts "to protect its networks and data from unauthorized access, data breaches, and intrusions." The Plan further stated that the FDIC intends to implement technologies to improve its ability to classify and protect sensitive data. Also, in 2017, the FDIC updated its IT strategic plan, revised its Breach Response Plan, and established a new Office of the Chief Information Security Officer. The FDIC also issued PIV cards to all employees and contractors and began requiring use of the cards to access FDIC computers. Looking ahead, the FDIC also plans to integrate cybersecurity into the FDIC-wide enterprise architecture and update its policies and procedures for expiring and outdated software and patch management. In addition, the FDIC is working to improve contingency planning in order to maintain or restore critical IT systems and applications during a disaster.

As global cyber intrusions continue to increase, the FDIC must continue to safeguard its own computer systems and data. The FDIC should ensure that IT and privacy program managers address weaknesses and build capabilities to prevent cybersecurity attacks, and minimize the risks associated with breaches, including the compromise of sensitive and PII data.

Utilizing Threat Information to Mitigate Risk in the Banking Sector

On February 12, 2013, the President issued Presidential Policy Directive 21 entitled, *Critical Infrastructure Security and Resilience*. This directive identified the banking sector as one of 16 critical infrastructure sectors that are vital to public confidence and the nation's safety, prosperity, and well-being. The President's National Infrastructure Advisory Council recommended and encouraged public and private sectors "to move actionable information to the right people at the speed required by cyber threats."[14] The FSOC, in its Annual Report (2017), also highlighted the importance of sharing threat information among the public and private sector as a "key priority" to reduce the risk of cybersecurity incidents and mitigate their impact if they occur.

The financial sector is diverse and interconnected, and spans from the largest institutions (assets greater than $2 trillion) to the smallest community banks. The International Monetary Fund in its Working Paper, *Cyber Risk, Market Failures, and Financial Stability* (2017), stated that "given the financial system's dependence on a relatively small set of technical systems, knock-on effects from downtimes and service disruptions due to successful attacks have the potential to be widespread and systemic." As identified by the FDIC in *Crisis and Response, An FDIC History 2008-2013*, financial system interconnectedness played a role in the financial crisis, "[e]ven financial institutions without large exposures to mortgage assets or derivatives were affected because they were deeply interconnected with the financial system in which these exposures played so significant a role."

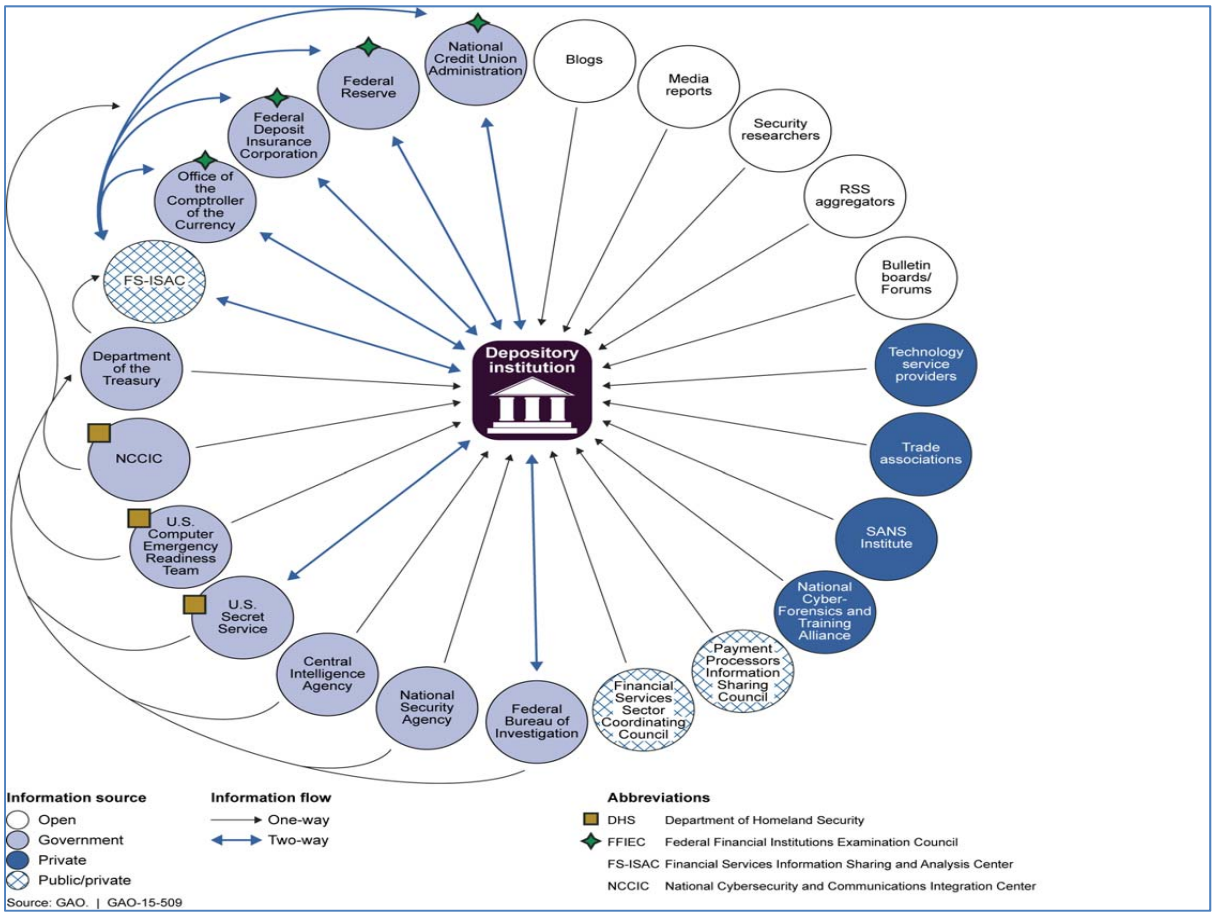
According to Presidential Policy Directive 21, the national preparedness systems must be integrated to secure critical infrastructure, withstand all hazards, and rapidly recover from disasters. Federal departments and agencies must collaborate with private sector critical infrastructure owners and operators. Both the Departments of the Treasury and Homeland Security recognized that sharing timely and actionable information is critical to managing risk.

In 2007, the Department of Homeland Security issued *the National Infrastructure Protection Plan* ("NIPP"); one portion of the NIPP relates to the financial sector – the *Banking and Finance Critical Infrastructure and Key Resources Sector-Specific Plan*. This Sector-Specific Plan described that financial regulators, including the FDIC, and the private sector are responsible for securing critical infrastructure, under the leadership of the Treasury Department. This relationship is addressed through several working groups and committees, including the Financial and Banking

[14] The President's National Infrastructure Advisory Council, *Securing Cyber Assets – Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017).

Information Infrastructure Committee ("FBIIC"),[15] the Financial Services Sector Coordinating Council ("FSSCC"),[16] and the Financial Services Information Sharing and Analysis Center ("FS-ISAC").[17] These organizations provide structures through which financial sector participants share information at the national and local levels, assess and mitigate sector-wide risks, develop and maintain key relationships, and conduct periodic testing of emergency protocols. The FDIC participates in these organizations to monitor cybersecurity, share information, and coordinate responses.

The U.S. Government gathers threat information about U.S. financial institutions and the financial system. For example, in its report entitled, Cybersecurity: *Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information* (2015), the GAO identified numerous sources of threat information that is provided to financial institutions.



[15] The FBIIC was created in 2001 to improve the reliability and security of the financial sector infrastructure and consists of 18 federal and state member organizations across the financial regulatory community.
[16] The FSSCC was established in 2002 to work collaboratively with key government agencies to protect the nation's critical infrastructure from cyber and physical threats and consists of 70 private sector members, including trade associations, financial utilities, and critical financial firms.
[17] The FS-ISAC was established in 1999 as a member-owned non-profit entity to share timely, relevant, and actionable physical and cyber security threat and incident information. FS-ISAC has 7,000 members across 39 countries.

As part of its review, GAO discussed the receipt of cyber threat information from the government with representatives from more than 50 depository institutions. The participants said that the information received from government sources was repetitive, not timely, and could not always be acted upon, because the information lacked sufficient details. Financial institutions said they rarely obtained cyber threat information from the government that they had not already received from other sources and that in some cases, smaller banks struggled with the volume of information from government agencies.

The GAO report also identified barriers to sharing threat information and reporting incidents in a timely manner. For example, institutions stated that information received from the government about cyber threats and actual attacks lacked sufficient context or details to allow institutions to take appropriate protective actions. In addition, some institutions were often reluctant or unable to share information with government agencies or other institutions, and expressed concern that the information shared could negatively impact their competitive advantages because reported information may become public. GAO also reported that classified information could not be shared with bank officials who did not have access to such information. As a result, intelligence community and law enforcement representatives were often cautious about declassifying certain information based on their concern that sensitive sources and methods used might be divulged.

In its Annual Report for 2017, the FSOC also recognized that there was a body of relevant information held by the government that was classified as national security information and must maintain its classification restrictions. Nevertheless, the FSOC encouraged agencies to "balance the need to keep information secure with efforts to share information with industry to enhance cybersecurity resilience." Therefore, the FSOC called on government agencies to "consider how to share information appropriately and, where possible, continue efforts to declassify (or downgrade classification) to the extent practicable, consistent with national security needs." Further, Federal Reserve Vice Chair for Supervision, Randal Quarles, recently stated that bank regulators have a bigger role to play in preventing cybercrime and should focus more on connecting financial institutions with national security agencies.[18] The former Comptroller of the Currency, Thomas Curry, also warned in his statement accompanying the agency's Semiannual Risk Perspective (Fall 2015) that "[w]e can't allow the federal banking system to be compromised by hackers or used by criminals or terrorists."

The financial sector also faces threats based on new technology; one worth noting in particular is the rapid growth of the virtual currency markets. According to Forbes, there are more than

[18] American Banker, *Regulators Have Bigger Role to Play in Cybersecurity* (December 1, 2017).

1,000 different virtual currencies with a total market value of $650 billion.[19] In addition, there has been widespread volatility in the marketplace. For example, CNN reported on December 9, 2017, that Bitcoin value soared from just under $10,000 per coin to more than $18,000 within one week. Clearinghouses and brokerages expressed concern about liability due to Bitcoin's high volatility and risk of manipulation because of the lack of transparency and regulation underlying Bitcoin futures products.[20]

Moreover, virtual currencies do not require the disclosure of information about a user's identity and therefore give participants some degree of anonymity. In the GAO's *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges* (2014) report, it noted that "[b]ecause some virtual currency transactions provide greater anonymity than transactions using traditional payment systems, law enforcement and financial regulators have raised concerns about the use of virtual currencies for illegal activities." The GAO further identified concerns about the use of virtual currencies in money laundering, financial and other crimes including cross-border criminal activities, and consumer protection issues related to the loss of funds on virtual currency exchanges.[21]

At present, the United States does not have a direct and comprehensive program to conduct oversight of the virtual currency markets. However, some government regulators and agencies have issued guidance to address concerns about virtual currencies, including the Financial Crimes Enforcement Network ("FinCEN"), Internal Revenue Service, Commodity Futures Trading Commission (CFTC), and Securities and Exchange Commission (SEC).[22] The FDIC has analyzed the potential impact that virtual currencies pose to financial institutions and formed a Financial Technology Working Group to monitor virtual currencies and other financial technology innovations. Among the challenges identified by the FDIC are the potential for illicit use and connection to criminal activity, legal and supervisory challenges, and integration with and risk to financial institutions. The FDIC should continue to monitor issues surrounding virtual currencies, to ensure that examiners and institutions are aware of the threats posed by these evolving technologies and markets.

Further, the Financial Services Sector-Specific Plan of the NIPP also described physical threats, such as natural disasters, terrorist attacks, and floods that have significant potential to disrupt the financial system. For example, CNN reported on November 10, 2017, *Hurricanes Could Bring*

---

[19] *2018 Will See Many More Cryptocurrencies Double In Value* (January 2, 2018).
[20] *Bitcoin to start futures trading, stoking Wild West worries*, Reuters (December 7, 2017).
[21] In the Statement of GAO's Director, Financial Markets and Community Investment before the Senate Committee on Banking, Housing, and Urban Affairs (September 12, 2017), GAO also identified data and privacy risks in the use of blockchain technology.
[22] FinCEN's *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* (FIN-2016-A005 October 25, 2016); *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets* (January 4, 2018*); SEC Chairman Jay Clayton Statement on Cryptocurrencies and Initial Coin Offerings* (December 11, 2017).

Another Disaster: Foreclosure, that approximately 4.8 million mortgaged properties were in the paths of Hurricanes Harvey, Irma, and Maria, representing nearly $746 billion in unpaid mortgage principal balances. Threats to financial institutions also may come from, or be exacerbated by, their dependence on other critical infrastructure services, such as energy, electricity, communication, and transportation. The recent hurricanes in Puerto Rico provide an example of the effect of the loss of electricity and transportation to the banking industry. During Hurricane Maria, banks lost electrical power to run their operations, and armored cars could not reach branches to stock ATMs due to road conditions.

Threat Information Critical to Financial Institutions and Their Service Providers. Threat information held by the U.S. Government is critical to financial institutions and their service providers. As discussed in FDIC's Supervisory Insights, *A Framework for Cybersecurity, "*financial institutions should have a program for gathering, analyzing, understanding, and sharing information about vulnerabilities to arrive at 'actionable intelligence.'" The Supervisory Insights article further stated that actionable intelligence can be gathered through a number of public and private resources, including FS-ISAC and the Department of Homeland Security's U.S. Computer Emergency Readiness Team. The FDIC, along with the FFIEC, has encouraged financial institutions to participate in FS-ISAC. Also, FDIC IT examiners assess an institution's process to gather threat information.

As noted in GAO's 2015 report referenced above, financial institutions are required to quickly respond to and mitigate the impact of data breaches. In order to secure their systems, institutions must have timely and actionable threat information. The 2015 Financial Services Sector-Specific Plan explained that "an incident impacting one firm has the potential to have cascading impacts that quickly affect other firms or sectors." The financial crisis provided an example of how the default of poorly underwritten mortgages at one bank rippled through the financial system to other banks, brokerages, and insurance companies through asset-backed securities and collateralized debt obligations backed by those mortgages.

Threat Information Critical to FDIC Examiners. Threat information held by the U.S. Government is also critical to FDIC examiners. Examiners should have access to relevant threat information and an understanding of the current threat level and types of threats, in order to focus examinations and prioritize areas for supervisory attention.

FDIC examiners use standard work programs to assess safety and soundness risk; however, they also have discretion to modify the scope of an examination and assess whether certain areas require greater scrutiny or expanded examination procedures. Therefore, understanding common threats across all institutions, even those not supervised by the FDIC, is important to

examiners. This information can be used by an examiner to test risk management programs at financial institutions. FDIC examiners should have relevant information concerning current threats and risks relating to an institution or a geographic region, which allows them to tailor examination procedures accordingly.

In addition, if examiners identify weaknesses in an institution's risk assessment process, including components related to gathering threat intelligence, they are instructed to identify such weaknesses in the Report of Examination. If the weaknesses are significant, an enforcement action may be used to specify and monitor the required corrective action. Further, FDIC examiners may initiate limited-scope examinations and visitations to investigate adverse or unusual situations based on up-to-date threat and risk information. These examinations and visitations have flexible formats. Examiners must assess whether bank staff have adequate threat information, and whether they take appropriate remediation action. Without relevant threat information, examiners may not be able to direct examination efforts effectively.

The FDIC, along with its government partners, collects and queries threat information contained within U.S. Government databases and repositories. The FDIC should continue to ensure that relevant threat information is disseminated to its examiner personnel to target risk areas at institutions and focus the FDIC's resources. The FDIC should also continue to assess whether financial institutions have access to and receive relevant threat information to mitigate risks. When institutions and examiners have threat information, they can more effectively take action to mitigate threats.

Readiness for Banking Crises

According to the Financial Crisis Inquiry Commission (2011),[23] nearly $11 trillion in household wealth vanished during the financial crisis that began in 2008. During the financial crisis, 4 million families lost their homes to foreclosure, and another 4-1/2 million slipped into the foreclosure process or were seriously behind on mortgage payments, and 26 million Americans were out of work, could not find full-time jobs, or gave up looking for work.[24] As reported in the FDIC's *Crisis and Response, An FDIC History, 2008-2013*, the net cost of the crisis was up to "roughly 80 percent of an entire year's gross domestic product."[25] The financial crisis resulted in 489 bank failures from 2008 through 2013. These failures cost the Deposit Insurance Fund ("DIF") approximately $72 billion, and it fell to the lowest level in history, a negative $20.9 billion by the end of 2009.[26] In addition, the number of problem banks peaked in early 2011 at almost 900, constituting nearly 12 percent of all FDIC-insured institutions.[27]

As this crisis unfolded, it challenged every aspect of the FDIC's operations, not only because of its severity, but also because of the speed with which problems unfolded. According to FDIC analysis, failure rates increased much faster during the 2008–2013 crisis than during the 1980s and early 1990s banking and thrift crises. For example, by 2009 almost 2 percent of banks had failed—a rate that was not reached in the previous crisis until the eighth year. In November 2017, the FDIC Chairman stated that "[i]t is also worth keeping in mind that the evolution of the global financial system towards greater interconnectedness and complexity may tend to increase the frequency, severity, and speed with which the financial crises occur."

The FDIC Chairman further remarked that "regulators must guard against the temptation to become complacent about the risk facing the financial system." The OFR noted in its Annual Report for 2017 that new vulnerabilities have emerged since the previous financial crisis and highlighted key threats to the financial system. There have been several changes in the financial markets since the crisis – for example: the increased use of automated trading systems, increased speed of executing financial transactions, and a wider variety of trading venues and

[23] The Financial Crisis Inquiry Commission was established by statute, Financial Enforcement and Recovery Act (2009), to "examine the causes of the current financial and economic crisis in the United States." The Commission was independent and composed of a 10-member panel of experienced financial experts knowledgeable in housing, economics, finance, market regulation, banking, and consumer protection. These members were selected by the leadership in Congress at the time.

[24] The Commission and staff reviewed millions of pages of documents, interviewed more than 700 witnesses, and held 19 days of public hearings. *See also*, U.S. Government Accountability Office, *Financial Regulatory Reform: Financial Crisis Losses and Potential Impact of the Dodd-Frank Act*, (February 2013).

[25] The FDIC conducted a study of the financial crisis entitled *Crisis and Response, An FDIC History, 2008-2013*, published in December 2017.

[26] Since the end of 2009, the DIF has grown every quarter and became positive in the second quarter of 2011. The DIF balance as of December 31, 2017 was $92.7 billion.

[27] The FDIC identifies "problem banks" as those with examination ratings of 4 or 5 (the two lowest ratings), which refers to institutions that exhibit deficiencies in practice or performance so severe that failure is either a distinct possibility (4 rating) or likely (5 rating) unless deficiencies are corrected.

liquidity providers. Vice Chair Quarles of the Federal Reserve Board stated that "the banking industry and technology firms have been seeking innovations in financial services that mirror and complement changes that have been made in other industries. Innovation is coming to finance with changes to consumer lending, financial advice, and retail payments, to name a few. . . . With a steady diet of news about the effect of electronic networks, personal devices, apps, and more on U.S. industries, many question the effect of these technologies on the payment system."[28]

The financial system continues to evolve with new risks and complexities, and such changes have the potential to create unanticipated risks. To carry out its program activities and meet its mission – and to prepare for the next banking crisis – the FDIC should ensure that its personnel and examiners have the proper skillsets. The FDIC has an effort underway to address succession planning and develop advanced subject-matter expertise.

The FDIC must continue to ensure that it has adequate plans in place to address disruptions to the banking system, irrespective of their cause, nature, magnitude, or scope. Further, its plans should be current and up-to-date, and incorporate lessons learned from past crises and the related bank failures. In addition, the plans should contemplate the present and foreseeable state of the banking and financial services sector, as banking industry practices and technologies continue to evolve. Also, the FDIC plans should continue efforts aimed at ensuring seamless coordination with and among other federal agencies and financial regulators, as well as with its international partners. The FDIC also should be able to react and respond quickly to a crisis. It should exercise and test its plans periodically to ensure that it is capable of fulfilling its mission, and ensure that its personnel and examiners have the proper skillsets to carry out program activities and meet the mission of the agency.

Authorities and Mechanisms. The FDIC must also continue to evaluate whether it has the proper authorities and tools in place for the next financial crisis. Since the previous crisis, the FDIC has been granted authority, pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"), to resolve the failure of systemically important financial institutions ("SIFI")[29] through orderly liquidation authority.[30] The FDIC must continue to ensure that it can execute these authorities effectively, especially with respect to the orderly liquidation authority. The FDIC continues to build upon its capabilities through monitoring of resolution

[28] Vice Chairman for Supervision Randal K. Quarles speech, *Thoughts on Prudent Innovation in the Payment System* (November 30, 2017).
[29] In *Resolution Plans: Regulators Have Refined Their Review Process but Could Improve Transparency and Timeliness* (April 2016), GAO defines a SIFI as a term "commonly used by academics and other experts to refer to bank holding companies with $50 billion or more in total consolidated assets and nonbank financial companies designated by the Financial Stability Oversight Council for Federal Reserve supervision and enhanced prudential standards, but the Dodd-Frank Wall Street Reform and Consumer Protection Act does not use the term."
[30] Orderly liquidation authority acts as a backstop where SIFIs cannot otherwise be resolved through Bankruptcy Code processes.

plans and pre-planning exercises with key stakeholders and international partners. However, planning for these activities is complex, and the processes remain untested.

The Dodd-Frank Act also gave the FDIC greater discretion to manage the DIF, including where to set the designated reserve ratio.[31] Consistent with the Act, the FDIC implemented a plan for the DIF by amending FDIC regulations to set the designated reserve ratio at 2 percent.[32]

The FDIC should also continue evaluating whether it has the proper mechanisms to address failing institutions in the next crisis. For example, the FDIC has used Shared-Loss Agreements ("SLA") to resolve failed institutions. In an SLA, a healthy acquiring institution agrees to purchase a failing institution, whereby the FDIC also agrees to absorb a significant portion of the losses experienced by the acquiring institution. According to the FDIC study on the financial crisis, SLAs were used by the FDIC for 62 percent of the failed banks and 82 percent of failed bank assets.[33] The FDIC study identifies a number of issues in its analysis of lessons learned – including exploring options for maintaining readiness in a low-failure environment, considering broadening its options for funding resolutions, and implementing the necessary back-office operations and infrastructure to oversee the loss share program. We have work planned to evaluate whether the SLAs utilized by the FDIC achieved its program goals effectively. The FDIC should explore whether there are other mechanisms that should be considered for the next financial crisis and ensure that such tools are ready to be implemented should they be needed.

When resolving a failing or failed bank, the FDIC uses an automated tool called the Claims Administration System ("CAS") to identify a depositor's insured and uninsured funds. When planning for the development of the CAS program, the FDIC expected that CAS could make insurance determinations for an institution of any size, up to 5 million deposit accounts; however, over time, the FDIC recognized the challenges of inconsistent and incomplete data at institutions. To mitigate these challenges, the FDIC issued a final rule on April 1, 2017 that required large institutions with greater than 2 million accounts to develop the capability to calculate deposit insurance coverage for their customers.[34] As of December 2016, this rule would cover 38 financial institutions that maintain between 2 million and 87 million deposit accounts, at an expected cost of approximately $478 million. The FDIC has used CAS to make insurance determinations for a failing bank with greater than 2 million accounts during pre-closing resolution planning but has not yet tested the system for institutions with greater than 2 million deposit accounts during a closing weekend. Accordingly, the FDIC is continuing to

[31] The reserve ratio is the DIF balance divided by estimated insured deposits.
[32] The FDIC stated in the background of the Final Rule on the Designated Reserve Ratio that "a fund that is sufficiently large is a necessary precondition to maintaining a positive fund balance during a banking crisis and allowing for long-term, steady assessment rates. 75 Fed. Reg. 79,286 (December 20, 2010).
[33] The failure of the Washington Mutual financial institution was not included in these figures, because of its size and unique characteristics.
[34] 12 C.F.R. Part 370.

upgrade CAS capacity and timeliness. We have ongoing work to assess to what extent CAS has achieved expectations for accuracy, timeliness, and capacity in making insurance determinations.

Staffing Plans. Determining the right number and skillsets of permanent staff needed to carry out and support the FDIC's program areas is a fundamental challenge. At the peak of the financial crisis in 2011, the FDIC maintained approximately 9,250 permanent, term, and temporary positions, whereas it's proposed staffing level for 2018 is 6,076 positions – a 34-percent reduction. The FDIC's annual budget is formulated primarily on the basis of an analysis of projected workload for each of the FDIC's business lines[35] and its program support functions.

Risk Management Supervision ("RMS"). With respect to RMS, the FDIC viewed its corps of experienced examiners as a great asset during the last financial crisis. However, much of the current FDIC workforce will transition into retirement over the next decade. According to FDIC data, more than 25 percent of the FDIC's current permanent workforce is projected to retire over the next 10 years, and many others are eligible to retire. While the FDIC has initiated a multi-year Workforce Development Initiative, it must maintain a steady flow of new examiners to step into the roles currently filled by seasoned examiners. In addition, the FDIC should ensure that there is a "knowledge transfer" from the more experienced personnel to the newer staff. To that end, RMS's strategic plan includes a goal to ensure that the knowledge, expertise, and experiences of its most tenured workforce are shared with and transferred to a less tenured workforce.

RMS uses a staffing model to forecast a range for the appropriate number of examiners and its overall staffing size. This staffing model has been validated on two prior occasions. However, as noted earlier, in periods of crisis, the number of problem banks typically increases. For example, in March 2011, the number of problem banks was 888, whereas it currently stands at approximately 100 (as of September 2017). These problem banks required additional attention from FDIC RMS examiners, because they had elevated safety and soundness risks. As a result, the risk management examination staff was 2,237 positions in 2011, and has now been reduced to 1,549 in 2018 — a 31-percent reduction. During the financial crisis of 2008-2013, the FDIC reduced specialty examinations, examiner training, and temporary assignments, and repurchased employees' annual leave, and hired temporary staff to address the increased workload. The FDIC also prioritized examination activities, increased staffing levels, and made greater use of off-site monitoring and on-site visitations between examinations.

[35] The FDIC has three major business lines: The Division of Risk Management Supervision ("RMS") for safety and soundness and IT examinations; the Division of Resolutions and Receiverships ("DRR") for failed bank resolutions and receivership activities; and the Division of Depositor and Consumer Protection ("DCP") to ensure financial institutions treat customers and depositors fairly.

Resolutions and Receiverships ("DRR"). DRR staffing requirements during the financial crisis were significantly higher than current staffing because of the bank failure workload. In 2010, there were 157 financial institutions that failed, as compared to only 5 failures in 2016 and 8 in 2017. As a result, DRR authorized staffing fell from 2,460 positions in 2010 to 409 positions in 2018 — an 83-percent reduction.

DRR has developed an operational readiness framework. The framework is composed of several elements, including resource management, operation training, knowledge management, contract management, operational governance (*i.e.*, delegated authorities, budget, and other organizational issues to address readiness), and technology support. The framework outlines a rapid hiring strategy through the use of contractors, retirees, and temporary employees. DRR has established number of contracts to support an increase in workload. The FDIC has determined that having the contracts in place minimizes the time to ramp up the acquisition process.

At the peak of the previous financial crisis, more than 80 percent of DRR staffing consisted of term and temporary employees. In 2005, the FDIC implemented a Corporate Employee Program ("CEP") that was designed to train new and experienced FDIC employees in a variety of functions, with the goal of creating a flexible workforce that could be re-allocated depending upon economic conditions and level of resolution activity. Subsequently, the FDIC determined that the CEP did not work as designed for augmenting DRR staffing needs, because it assumed that many of the employees who would be shifted to resolution tasks would come from the supervision division. However, as resolution activity began to increase, the workload of other divisions—including supervision—also increased, so that the realignment of resources could not be achieved as intended.

Other Challenges to FDIC Staffing Issues. The staffing challenges identified above are difficult to address quickly within a compressed timeframe, because the FDIC requires background investigations before hiring new employees. The FDIC requires that employees, appointees, and applicants for employment undergo a National Agency Check and Inquiry with Credit or other appropriate background investigation according to the positions they hold. Background investigations are critical to ensure that the FDIC employs and retains only those persons who meet all federal requirements for suitability (*i.e.*, character, reputation, honesty, integrity, trustworthiness) and whose employment or conduct would not jeopardize the accomplishment of the FDIC's duties or responsibilities. A high-quality suitability program is essential to minimizing the risk of unauthorized disclosures of sensitive information and to helping ensure that information about individuals with criminal backgrounds or other questionable behavior is identified and assessed as part of the process for granting or retaining

clearances. Our OIG evaluation, *The FDIC's Personnel Security and Suitability Program*, examined the timeliness of background checks for FDIC personnel. We found that during the period of 2011 to 2013, the submissions from the FDIC to investigate the background of employees and contractors exceeded OPM's 14-day requirement, and that the average delays extended nearly 2 months.

According to the Division of Administration's ("DOA") Acquisition Services Branch ("ASB"), ASB initially had difficulty recruiting and hiring term employees at the beginning of the most recent financial crisis. It appeared that prospective candidates were not interested in such term-limited appointments. However, as the crisis persisted, ASB expanded the number of permanent positions, reorganized, and was able to attract candidates for term appointments and complete contracting requirements.

In addition, the current Administration has requested that government agencies develop reform plans aimed at reducing staffing levels. In June 2017, the FDIC submitted its multi-year strategy used to reduce operating and staffing on an annual basis to the OMB. The FDIC indicated in its submission that from 2010 through 2017, it had reduced its annual budget by approximately 46 percent and it's staffing by 30 percent. The FDIC anticipates a permanent workforce of no more than 6,000 in the near term but noted that adjustments may be necessary.

Readiness of Support Functions. In addition to staffing models, the FDIC should also ensure that it has the proper infrastructure in place, in order to address the administrative functions of the agency in a timely manner during the next banking crisis. For example, the FDIC must ensure that it has the proper contracting services in place. During the recent financial crisis, the FDIC issued over 6,000 awards totaling more than $8 billion. The vast majority of these awards went to support resolution and receivership activity at FDIC headquarters and in the Dallas Regional Office. In addition to the contracting activity, the FDIC should also ensure that it has the proper support services for such contracts, including legal support (Legal Division), as well as oversight managers and technical monitors. In addition the FDIC should ensure that it has the proper level of human resources personnel to hire new employees and annuitants. The agency should continue to ensure that there is sufficient IT equipment (including computers, servers, peripheral devices, software licenses, and communications devices) in preparation for the next financial crisis, and a robust infrastructure so that these computer systems may operate in a secure environment.

The FDIC must continue to maintain and update its readiness strategies, and test and exercise its plans to ensure they keep pace with an ever-changing financial environment and incorporate important lessons from the past.

Enterprise Risk Management Practices

Enterprise Risk Management ("ERM") is a decision-making tool that assists federal leaders in anticipating and managing risks at an agency, and helps to consider and compare multiple risks and how they present challenges and opportunities when viewed across the organization. According to OMB guidance, ERM is beneficial because it addresses a fundamental organizational issue: the need for information about major risks to flow both vertically (*i.e.*, up and down the organization) and horizontally (*i.e.*, across its organizational units) to improve the quality of decision-making. When implemented effectively, ERM seeks to open channels of communication, so that managers have access to the information they need to make sound decisions. ERM can also help executives recognize how risks interact (*i.e.*, how one risk can exacerbate or offset another risk). Further, ERM examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance. ERM encompasses many risk areas, including financial risk, operational risk, reporting risk, compliance risk, governance risk, strategic risk, and reputational risk.

In July 2016, OMB issued an updated Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, to ensure that federal officials effectively manage risks that could affect the achievement of agency strategic objectives.[36] OMB Circular A-123 requires agencies to integrate risk management and internal control functions and guides agencies' processes to integrate organizational performance and ERM. The Circular emphasizes the need for agencies to coordinate risk management and strong and effective internal controls into existing business activities as an integral part of governing and managing an agency.

OMB defines the following terms:

- **Risk.** The effect of uncertainty on objectives.
- **Risk management.** A series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives.
- **Enterprise Risk Management.** An effective agency-wide approach to addressing the full spectrum of the organization's significant internal and external risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos.

Source: OMB Circular A-123

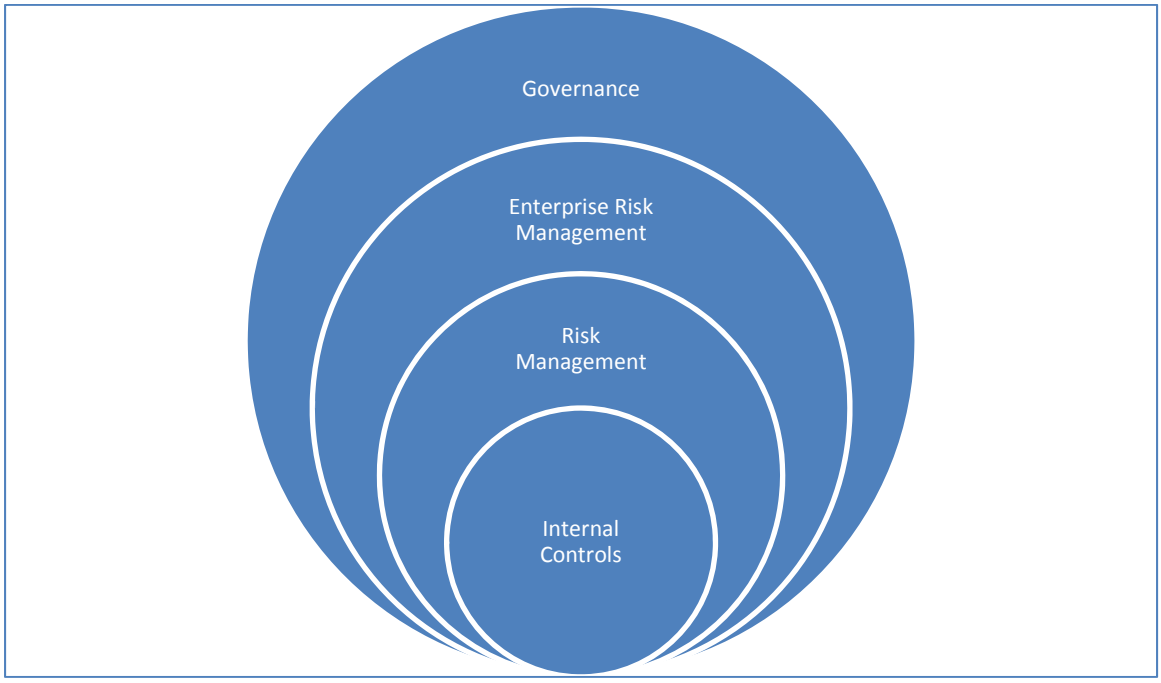
OMB Circular A-123 encouraged agencies to establish a Risk Management Council ("RMC"); develop "Risk Profiles", which identify risks arising from mission and mission-support operations;

[36] The FDIC has determined that while Circular A-123 is not binding on the FDIC, the Circular provides "good government" principles that may be useful to the FDIC's own ERM program.

and consider those risks as part of the annual strategic review process. An effective RMC includes senior officials from program operations and mission-support functions to ensure the identification of risks that have the most significant impact on the mission outcomes. The Chief Operating Officer ("COO") or a senior official with responsibility for the enterprise should serve as RMC chairperson.

OMB Circular A-123 complements OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, Section 270, which discusses agency responsibilities for identifying and managing strategic and programmatic risk as part of agency strategic planning, performance management, and performance reporting practices. Together, these two OMB Circulars constitute the ERM policy framework for the federal government. OMB views ERM as part of the overall governance process, and internal controls as an integral part of risk management and ERM.

The Relationship Between Internal Controls and ERM

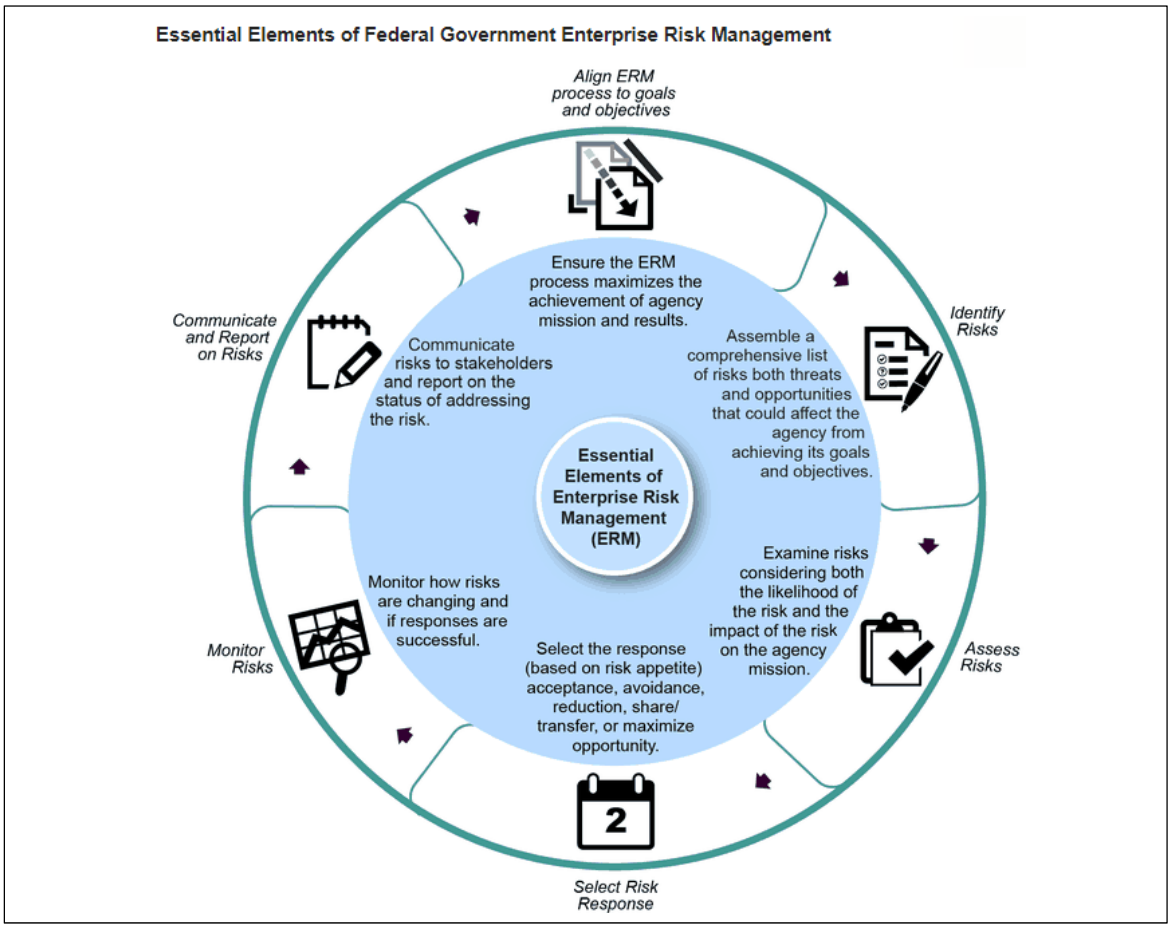


Source: OMB Circular A-123.

OMB Circular A-123 specifies elements that federal agencies' ERM frameworks should include and steps agencies should take to develop these frameworks. These include a planned risk management governance structure, a process for considering risk appetite and risk tolerance levels, a methodology for developing a risk profile, a general implementation timeline, and a plan for developing the depth and quality of the risk profiles over time. The organization's senior leadership should establish a risk appetite (*i.e.*, amount of risk an organization is willing to accept), which serves as a guidepost to establish strategy and select objectives, and a risk

tolerance (*i.e.*, an acceptable level of variance in performance relative to the achievement of objectives).

GAO reported that effective ERM implementation starts with an agency establishing a customized ERM program that fits its specific organizational mission, culture, operating environment, and business processes.[37] GAO identified six essential elements to assist federal agencies as they move forward with ERM implementation.



Source: GAO-17-63.

In our 2008 report, *The FDIC's Internal Risk Management Program*, we evaluated the extent to which the FDIC's implementation of an ERM program complied with applicable government-wide guidance. We found that the FDIC should institutionalize how the various FDIC committees interrelate and support ERM, and ensure the continuity of risk management efforts as changes in leadership and/or senior management occur. Since that report, the FDIC has taken steps described below to develop an ERM framework, but in light of recent organizational

[37] *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk* (December 2016).

changes to the program, the FDIC must continue to enhance and develop its ERM infrastructure to achieve an effective and efficient ERM program.

ERM is especially important for the FDIC at this time since it is experiencing significant changes at its senior levels, including the Board of Directors[38] and its governance bodies. The FDIC has a Board with five members: the FDIC Chairman, the FDIC Vice Chairman, the Director of the Consumer Financial Protection Bureau ("CFPB"), the Comptroller of the Currency, and an internal FDIC board member. The FDIC Chairman's term expired in November 2017, but he continues to serve as Chairman until a nominee is confirmed. The Vice-Chairman's term expires in April 2018. The Comptroller of the Currency was appointed in November 2017, and the CFPB Director is currently in an acting role. In addition, the FDIC internal board member position has been vacant since June 4, 2015.

In 2010, the FDIC engaged a consulting firm to evaluate its existing risk management practices and recommend improvements. The consulting firm identified several gaps in the FDIC's risk management structure. For example, most risks at the FDIC were addressed within existing hierarchical organizational structures, with limited communication across the agency organizational units. Further, while the FDIC had a network of internal committees to address various risks, governance over those committees was ambiguous. The consultant recommended the establishment of a centralized, independent risk management organization headed by a Chief Risk Officer ("CRO") that should report directly to the FDIC Chairman.

In January 2011, the FDIC Board of Directors established the CRO position and subsequently, in December 2011, the FDIC Board approved the creation of an Office of Corporate Risk Management ("OCRM") with staffing of 15 employees. The CRO reported operationally to the FDIC Chairman and functionally to the Board of Directors. The OCRM provided an organization within the FDIC to review external and internal risks with a system-wide perspective and instill risk governance as part of the FDIC's culture. In addition, the FDIC established an Enterprise Risk Committee ("ERC") chaired by the CRO. The newly established ERC evaluated significant external business risks facing the FDIC and banking industry.

The first CRO assumed his position in August 2011 and the OCRM staffing was authorized at 15 positions. The initial CRO retired in May 2016 and the then-Deputy CRO became the Acting CRO until his retirement in June 2017. Further, due to other staff departures, there were only five professional staff in OCRM by September 2017.

[38] According to the Federal Deposit Insurance Act, the management of the FDIC is vested in a Board of Directors consisting of five members who each serve 6-year terms – the Comptroller of the Currency, the Director of the Consumer Financial Protection Bureau, and three members appointed by the President with advice and consent of the Senate. 12 U.S.C. §1821(a) and (b). The three members are the Chairman of the FDIC, the FDIC Vice Chairman, and an internal FDIC Director.

In September 2017, the FDIC transferred OCRM functions into the Division of Finance ("DOF"). The reorganization combined the OCRM and the Corporate Management Control ("CMC") Branch into a newly-constituted Risk Management and Internal Controls Branch ("RMIC") within DOF. The title of CRO will now be held by a Deputy Director in DOF. Currently, the Acting Deputy Director heads RMIC. The FDIC plans to select a permanent CRO in early 2018. As part of the 2017 reorganization, the FDIC also decided to use the existing Operating Committee as the focal point for the coordination of risk management at the FDIC, thus disbanding and replacing the ERC. The FDIC also maintains a framework to enhance awareness of external threats that may impact FDIC operations. The framework consists of Regional Risk Committees that review regional economic and banking trends; the Management Risk Roundtable that examines risks to the banking industry and the Deposit Insurance Fund; and the External Risk Forum that facilitates information sharing and awareness of risks facing the banking industry and the FDIC. We intend to conduct an evaluation of the effectiveness of the FDIC ERM Program.

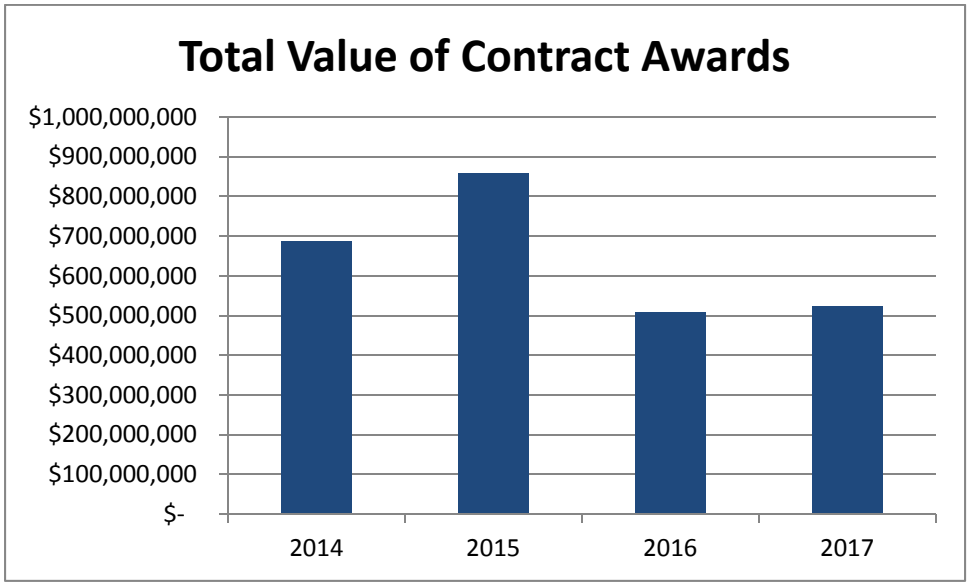
The FDIC should continue institutionalizing ERM and best practices outlined in OMB guidance. The FDIC Board of Directors, senior management, and individuals at every level throughout the FDIC should acknowledge, understand, and take ownership of current and emerging risks to the FDIC mission and be prepared to take steps to mitigate these risks.

Acquisition Management and Oversight

According to the GAO's *Framework for Assessing the Acquisition Function at Federal Agencies* (2005), agencies should effectively manage their acquisition process in order to ensure that contract requirements are defined clearly and all aspects of contracts are fulfilled.[39] GAO noted that clear descriptions of contract requirements lead to the acquisition of goods and services at a fair price. Vague statements of work, however, can lead to miscommunication, uncertainty, delays, and increased costs. Agencies must properly oversee contractor performance and identify any deficiencies, as well ensure appropriate verification of expenditures.

Over the last 10 years (2008 through 2017), the FDIC awarded more than 12,600 contracts totaling nearly $11.2 billion. The DOA ASB provides a wide range of contracting programs and services to support day-to-day operations at the FDIC. As shown in the chart below, the FDIC awarded $2.6 billion in contracts from January 2014 to December 2017. In addition, the FDIC budget for 2018 includes more than $457 million in contracting expenses for outside services.

FDIC Contract Awards January 2014-December 2017



Source: FDIC Division of Administration

Three divisions, DOA, the Division of Information Technology ("DIT"), and DRR, accounted for 96 percent ($2.5 billion) of all contract awards through DOA's ASB between January 2014 and December 2017. DOA contracts for services such as security, facilities, and records management. DIT procures contracts for technology services, such as help desk personnel,

[39] GAO, *Framework for Assessing the Acquisition Function at Federal Agencies* (2005); *See also*, Testimony of GAO Assistant Comptroller General before the Subcommittee on Oversight and Investigations, U.S. House of Representatives (December 3, 1992).

computer systems design, and telecommunications. DRR is responsible for managing the resolution process, which involves a range of contracts to support the closing functions at failed institutions, and management and disposition of receivership assets. For example, DRR contracts include appraisal management services, credit card consulting, commercial loan servicing, and data management.

Contracting Officers are responsible for ensuring the performance of all actions necessary for efficient and effective contracting, compliance with contract terms, and protection of the FDIC's interests in all of its contractual relationships. In addition, FDIC program offices develop contract requirements, and program office Oversight Managers and Technical Monitors oversee the contractor's performance and technical work. Oversight management involves monitoring contract expenses and ensuring that the contractor delivers the required goods or performs the work according to the delivery schedule in the contract. In *Crisis and Response, An FDIC History, 2008-2013*, the FDIC explained that contracting was an essential part of the FDIC's failure resolution process during the financial crisis, but it was overtaxed early in the crisis. Specifically, staffing was thin, contract timeframes to approve new contracts or modify existing contracts were too long to support the volume of failures, and the FDIC had to rapidly hire and train Oversight Managers. We are initiating an evaluation to review FDIC's current contract oversight program.

The FDIC also must continue to ensure that its contractors and contracting personnel meet security and suitability standards for employment and access to sensitive information. In addition, contractors must meet criteria for integrity and fitness such as conflicts of interest, ethical responsibilities, and use of confidential information.[40] These security protections are important since the contractors have access to FDIC space and information and use FDIC equipment. Such information includes sensitive information related to bank closings as well as personally identifiable information for private citizens and FDIC employees. DOA's Security and Emergency Preparedness Section, Personnel Security Unit, is responsible for establishing and implementing contractor personnel security policy, including evaluations, adjudications, approvals, and clearances, and ensuring appropriate background investigations are conducted on contractor personnel.[41]

With regard to contracting for legal services, for the 4 years from 2014 through 2017, the FDIC's Legal Division spent $364 million on outside counsel. The Legal Division has independent contracting authority and is excluded from FDIC procurement policies executed by ASB. The Legal Division contracts for services of outside counsel in areas such as bankruptcy and creditor's rights; collections; environmental law; federal, state, and local taxation; foreclosures;

[40] 12 C.F.R. Part 366.
[41] FDIC Circular 1610.2, *Personnel Security Policy and Procedures for FDIC Contractors*.

real estate; and financial transactions. The Legal Division retains outside counsel through Legal Services Agreements that contain terms and conditions applicable to referrals of FDIC legal matters. The Legal Division assigns an Oversight Attorney ("OA") responsible for all strategic and major tactical decisions associated with a matter. The OA also monitors progress against a case plan and budgets.

The FDIC characterizes "large contracts" as those with award amounts exceeding $20 million or that require greater oversight based on the complex nature of the contract. As of January 2018, the FDIC had 11 large contracts between $20 and $112 million in value. Over the past 2 years, DRR and DIT oversaw a total of 540 contracts, each with a value of $1 million or more.

In our OIG work, we have noted several shortcomings in contractor oversight, which can lead to delays and cost overruns. In our report, *The FDIC's Failed Bank Data Services Project* (March 2017), we reviewed a 10-year, $295 million project related to the transition of the management of failed financial institution data from one contractor to another. Our review focused on transition costs of approximately $24.4 million. The audit concluded that transition milestones were not met, resulting in a one year delay. Further, transition costs, while less than projected in the approval, were greater than the initial estimates at contract inception, by $14.5 million. We concluded that the reasons for the increase were 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 the solicitation. Further, the FDIC did not establish clear expectations in the contract documents and did not implement a project management framework and plans.

In addition, our OIG report on the *FDIC's Identity, Credential, and Access Management Program* (2015), reviewed the FDIC's Identity, Credential, and Access Management Program ("ICAM") and identified significant issues or program risks. We found that the FDIC had not achieved its goal of issuing identity credentials (known as personal identity verification (PIV) cards) to all eligible employees and contractor personnel. The FDIC had not established appropriate governance to ensure the ICAM program's success. The FDIC awarded an initial contract for $3.4 million to procure expertise and support for planning and implementing the credential program. We reported that the milestone goals for this project slipped by more than 2 years (from August 2014 to December 2016) and that the contract cost ceiling needed to be increased by $1.5 million — a 44 percent increase. We determined that these delays and cost overruns were the result of technical hurdles as well as unclear roles and responsibilities of the parties involved in governing the ICAM program.

In 2017, we conducted a *Follow-on Audit of the FDIC's Identity, Credential, and Access Management Program* (June 2017) and found that the FDIC addressed the issues from the 2015 report but experienced considerable challenges that warranted management's attention. For example, the FDIC had not established policies and procedures governing the management and use of PIV cards for physical and logical access. We also concluded that the FDIC did not maintain current, accurate, and complete contractor personnel data needed to manage PIV cards, and management had not finalized and approved a plan for retiring the FDIC's legacy PIV card system.

In response to recommendations made in OIG reports, the FDIC is taking actions to improve contract management and oversight. For example, 346 Oversight Managers and Technical Monitors received training, and ASB was developing an Oversight Manager refresher course during 2017.

In a time of reduced budget and staff, the FDIC should continue efforts aimed at optimizing its use of contract resources by clearly defining work and deliverables, managing contract milestones, and overseeing contract expenditures. Taking those steps helps to ensure that the FDIC receives goods and services at a fair price and without undue delays and costly inefficiencies.

Measuring Costs and Benefits of FDIC Regulations

GAO's report, *Dodd-Frank Act Regulations: Implementation Could Benefit from Additional Analyses and Coordination* (2011), recognizes that, while not required, many Federal financial regulators generally perform cost-benefit analysis when they propose a new rule. The Congressional Research Service ("CRS") has recognized that the use of cost-benefit analysis may improve the quality and effectiveness of federal rules and minimize burden in its *Cost-Benefit and Other Analysis Requirements in the Rulemaking Process* (2014).

On February 3, 2017, the President issued Executive Order 13772 that set forth seven core principles for Federal regulations governing U.S. financial institutions, including "make regulation[s] efficient, effective, and appropriately tailored." As required by this Executive Order, the Department of the Treasury issued a report, *A Financial System That Creates Economic Opportunities* (June 2017), examining costs relating to compliance with regulations imposed on banks. This report recommended that financial regulatory agencies should conduct rigorous cost-benefit analysis and make greater use of proposed rulemaking to solicit public comment. While there is no formal requirement for financial regulators to conduct cost-benefits analysis for rulemaking, the FDIC generally conducts this analysis on its own initiative for proposed rules. In addition, the FDIC routinely solicits comments from the public for Notice of Proposed Rulemakings in accordance with the provisions of the Administrative Procedures Act , and because of the difficulty in obtaining quantitative data measuring regulatory costs and benefits, it considers such comments to be an important source of information.

The FDIC has developed a framework for conducting analysis of regulations. According to the FDIC's *Statement of Policy on Development and Review of FDIC Regulations and Policies* (updated December 2017), the agency "evaluate[s] benefits and costs based on available information, and consider[s] reasonable possible alternatives; the main alternatives should be described and analyzed for consistency with statutory or regulatory objectives, effectiveness, and burden on the public or industry." Also, in 2015, the FDIC organized an Office of the Chief Economist and Regulatory Analysis within the Division of Insurance and Research, which, according to the FDIC, aims to provide consistency and rigor in its regulatory analysis.[42]

The CRS report, *Cost Benefit Analysis and Financial Regulator Rulemaking* (2017), recognized that performing cost benefit analysis "can be useful in determining whether or not a regulation is beneficial. However, performing CBA [Cost Benefit Analysis] can be a difficult and time-consuming process, and it produces uncertain results because it involves making assumptions

[42] The Federal Reserve also recently established a new office to analyze the impact of its regulations. (See *Fed adds staff for new office dedicated to gauging economic impact of regulations*, Politico Pro, January 18, 2018).

about future outcomes." The CRS report also noted that cost benefit analysis, "for financial regulation is particularly challenging, due largely to the high degree of uncertainty over precise regulatory costs and outcomes." The report identified three challenges to making accurate cost benefit analysis: (1) behavioral changes of people as they adapt to a new regulation, (2) quantification that must overcome uncertainty over the causal relationship between the regulation and outcomes, and (3) monetization, which is difficult for outcomes that do not have easily discernable monetary values.

In addition, the Yale Law Journal published a review entitled *Cost-Benefit Analysis of Financial Regulations Case Studies and Implications* (2015), which examined select financial regulations. This review determined "that the capacity of anyone . . . to conduct qualified [Cost Benefit Analysis on Financial Regulations] with any real precision or confidence does not exist for important, representative types of financial regulation." The review concluded that, "[t]oo many contestable assumptions are required for anyone producing or consuming guesstimate [Cost Benefit Analysis on Financial Regulations] to have any confidence in any specific estimate of costs or benefits, even if expressed in ranges or bounds."

Another CRS report, *An Analysis of the Regulatory Burden on Small Banks* (2015), noted that bank regulators, including the FDIC, generally did not quantify overall costs or benefits for 14 major rules issued in accordance with the Dodd-Frank Act requirements, although regulators did assess some costs associated with individual rules. The bank regulators quantified some costs for two rules and qualitatively discussed costs and benefits for three rules. The CRS did not identify any cost-benefit analysis for the other remaining rules.

Similarly, GAO's report, *Dodd-Frank Regulations: Agencies' Efforts to Analyze and Coordinate Their Recent Final Rules* (2016), reviewed five major rules, one of which was issued by the FDIC, and found that regulators quantified some costs in all five rules. The FDIC rule was one of the two where some benefits were quantified. GAO cited earlier work that noted that bank regulators faced difficulties in quantifying benefits because financial regulatory concepts are complex and challenging to define and model; research methodologies do not necessarily address economic values and the distribution of risk; and flows of future costs and benefits can be uncertain and difficult to project.[43] For these reasons, the FDIC faces challenges with proper data collection and lack of available information with respect to measuring costs and identifying benefits for a particular rule.

In responses to the GAO report, regulators advised GAO that there are industry concerns about the potential for unintended consequences from Dodd-Frank Act rulemaking and

[43] *Dodd-Frank Regulations: Regulators' Analytical and Coordination Efforts* (2014).

implementation and were undertaking retrospective reviews of rules. For example, in February 2016, the FDIC issued a proposed rule on *Recordkeeping for Timely Deposit Insurance Determination*. The FDIC experienced challenges in quantifying the costs and benefits of this rule. The FDIC had engaged an independent contracting firm to estimate the expected costs that 36 large banks would incur as a result of the proposed rule requiring such banks to calculate insured deposits within 24 hours of failure. The contractor estimated that the cost to the industry was $328 million (80 cents per deposit account). The FDIC found, however, that the benefits of the rule were difficult to determine, explaining that "[b]ecause there is no market in which the value of these public benefits can be determined, it is not possible to monetize these benefits."

During the comment period for this rule, the American Bankers Association, Clearinghouse Association, Consumer Bankers Association, and Securities Industry and Financial Markets Association provided comments that outlined numerous concerns about the proposed rule. One such concern was that the FDIC had not adequately considered the costs the rule would place on financial intermediaries, the disruption that it would cause in deposit markets, and the risk that it would place on the security of depositors' personal information. The associations further stated that the FDIC contractor had underestimated the actual implementation costs of the rule and did not contemplate ongoing costs to the institutions. In addition, the associations asserted that the FDIC did not fully consider that the increased costs would likely be passed on to customers at the institutions. They also noted that "the FDIC has a responsibility to provide concrete evidence to support the purported benefits" of the rule and "conduct a full-fledged cost-benefit analysis."

After evaluating public comments on the proposed rule, the FDIC issued a final rule with a revised total cost of $478 million in which the cost to the covered institutions was estimated at $368 million with the remaining costs accrued to depositors and the FDIC. In the final rule, the FDIC stated that the rule would ensure "prompt and efficient deposit insurance determinations by the FDIC and thus the liquidity of deposit funds; enabl[e] the FDIC to more readily resolve a failed [Insured Depository Institution]; reduc[e] the costs of failure of a covered institution by increasing the FDIC's resolution options; and promot[e] long term stability in the banking system by reducing moral hazard." The FDIC further advised us that the estimated costs of implementation would amount to less than one seventh of one percent of 2015 total noninterest expenses for institutions required to implement the rule.

The FDIC engages in a regulatory review process at least every 10 years, in accordance with the Economic Growth and Regulatory Paperwork Reduction Act. This process considers whether any of the FDIC's regulations are outdated, unnecessary, or unduly burdensome. In addition, in

2009, the FDIC established an Advisory Committee on Community Banking to provide advice and guidance on policy issues impacting small community banks, including current examination policies and procedures, credit and lending practices, deposit insurance assessments, insurance coverage, and regulatory compliance, including the cost and benefit of regulations. Community banks include rural and urban institutions supervised by the FDIC. Further, in 2012, the FDIC conducted a Community Banking Study to identify and explore issues and questions about community banks. The Study found a number of areas warranting additional FDIC research, including how regulatory costs for community banks have changed. As part of its Annual Performance Plan for 2017, the FDIC committed to follow up on issues identified in the Study relating to efficiency, consistency, and transparency of its supervisory processes.

While the FDIC aims to conduct cost-benefit analyses for proposed rules, it faces challenges in collecting the necessary data and information, and estimating the costs and benefits of its regulations with a degree of precision. The FDIC should continue efforts to make meaningful cost-benefit determinations because regulations have lasting effects on institutions and consumers.