The FDIC's Implementation of Enterprise Risk Management

July 2020 **EVAL-20-005**

Evaluation Report

Program Audits and Evaluations

☆☆☆☆☆☆☆☆

Office of Inspector General

Executive Summary

The FDIC's Implementation of Enterprise Risk Management

Enterprise Risk Management (ERM) is an agency-wide approach to addressing the full spectrum of internal and external risks facing an agency. ERM provides an enterprise-wide view of challenges that enables agencies to effectively allocate resources, prioritize and proactively manage risk, improve the flow of risk information to decision makers, and work towards successful accomplishment of their missions. ERM ensures transparency and accountability in business practices, reporting, and governance, which can improve stakeholder confidence in the agency's work. To achieve these benefits, ERM should be integrated into the culture of the agency.

The FDIC Board of Directors has designated the Operating Committee (OC) as the "focal point" for the coordination of risk management at the FDIC. The FDIC further designated the OC as the FDIC's Risk Management Council (RMC) and the oversight body for ERM. The OC is comprised of Division and Office Directors and Deputies to the Chairman.

The FDIC's Division of Finance, Risk Management and Internal Controls Branch (RMIC), is responsible for implementing the FDIC's ERM program. With the establishment of RMIC, the FDIC has made progress toward implementing ERM in compliance with government-wide guidance and best practices. RMIC works with the FDIC's risk committees and Divisions and Offices to identify, assess, and mitigate internal and external risks. RMIC seeks to maintain a coordinated framework for risks to the enterprise and increase awareness of emerging risks. Accordingly, it aims to align resources, processes, policies, and procedures, to address key risks.

Our evaluation objective was to assess the FDIC's implementation of ERM against relevant criteria and best practices. We assessed the FDIC against those best practices that, in our professional judgment, aligned with the structure of the Agency and the FDIC's decision to use the OC as its RMC.

Results

We found that the FDIC needs to establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. This will help ensure that the FDIC integrates ERM into its culture, practices, and capabilities so that risks across the enterprise are considered and prioritized as part of operations support, program management, budget decisions, and strategic planning. For example, we found that the FDIC did not establish clear ERM oversight authorities, roles, and responsibilities for the OC as recommended by relevant criteria and best practices. Specifically, the FDIC did not clearly articulate in its policies and procedures how the OC, as the FDIC's designated RMC, performs the following responsibilities:

- Oversight of the establishment of the FDIC's risk profile;
- Oversight of the assessment of risks;
- Oversight of the development of risk responses; and the
- Final determinations of the approaches and actions to address the risks included in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

As a result, it is not clear if the OC is performing these responsibilities and how it is doing so. Carrying out these responsibilities would ensure the range of risks facing the FDIC and their mitigation strategies are prioritized and overseen at the enterprise level by senior officials responsible for program operations and mission support.

We also found that the FDIC did not clearly define the roles, responsibilities and processes of the committees and groups involved in ERM. Specifically, the FDIC did not:

- Ensure that the FDIC Board of Directors (Board) endorses the risk appetite statement prior to its issuance;
- Ensure effective communications to the Board relating to ERM;
- Ensure that the Board understands its role with respect to ERM at the FDIC;
- Develop procedures to specify how risk committee activities are to be accomplished and how they interface with other ERM processes;
- Require documentation of meetings of the various risk committees; and
- Update and memorialize ERM processes for RMIC, Divisions, and Offices.

Having well-defined authorities, roles, and responsibilities for ERM will help to ensure that the range of risks facing the Agency and banking sector are properly identified and managed. If risks are not considered by officials with appropriate knowledge and experience, the FDIC may not prioritize and address the risks that have significant impact on the Agency and the banking sector. Without a clear governance structure over ERM, the FDIC cannot ensure that ERM will fully mature and be integrated into the agency and its culture. Integrating ERM leads to improved decision-making and enhanced performance.

Recommendations

Our report contains eight recommendations for the FDIC to: (1) define, document, and implement the authorities, roles, and responsibilities of the OC as the RMC; (2) define the roles and responsibilities of the Board, including its role in endorsing the risk appetite statement; (3) develop and implement ERM communication protocols to the Board; (4) define the roles and responsibilities of each committee in relation to ERM; (5) develop and implement procedures on how the risk committees interface with other ERM processes; (6) record meeting minutes of the OC and other relevant risk committees; (7) develop and implement procedures pertaining to how the Divisions, Offices, and RMIC should execute their particular job functions related to ERM; and (8) define, document, and implement procedures to ensure that enterprise risks are evaluated using ERM before enterprise-wide decisions are made.

The FDIC concurred with five and non-concurred with three of the eight recommendations made in this report.

Contents

Federal Deposit Insurance Corporation
Office of Inspector General
Office of Program Audits and Evaluations

July 8, 2020

Subject | ***The FDIC's Implementation of Enterprise Risk Management***

Federal government leaders manage complex missions that have risks across their organizations. Enterprise Risk Management (ERM) is a tool that can assist Federal leaders in anticipating, planning for, and managing risks. It can also help leaders understand the interrelationships among multiple risks in their agency and how they present challenges and opportunities when examined as a whole. ERM seeks to understand the combined impact of internal and external risks as a portfolio across the organization, rather than managing risks only within silos. ERM balances risks and returns, so that an agency increases its ability to achieve its strategic objectives.

ERM provides an enterprise-wide view of challenges that enables agencies to effectively prioritize and proactively manage risk, allocate resources efficiently, improve the flow of risk information to decision makers, and work towards successful accomplishment of their missions. Effective ERM facilitates improved decision-making through a structured understanding of opportunities and threats. ERM addresses a fundamental organizational issue: the need for information about major risks to flow both up and down the organization and across its organizational structures to improve the quality of decision-making.

Pursuant to the Resolution of the Board of Directors (September 2017), the FDIC's Operating Committee (OC) was designated the "focal point" for the coordination of risk management at the FDIC. The FDIC further designated the OC as the FDIC's Risk Management Council (RMC) and the oversight body for ERM. The FDIC's Division of Finance, Risk Management and Internal Controls Branch (RMIC), is responsible for implementing ERM at the FDIC. RMIC works with FDIC Divisions and Offices to identify and address internal and external risks. According to FDIC Directive 4010.3 entitled Enterprise Risk Management and Internal Control Program (October 25, 2018), the FDIC seeks to ensure that it:

- Has increased awareness of emerging key risks and an opportunity to address them before they occur;
- Properly aligns resources, processes, policies, and procedures to adequately address key risks;
- Establishes and maintains a coordinated framework for capturing, sharing, and reporting risk to FDIC leadership and developing appropriate solutions; and
- Establishes and integrates internal control into its operations.

Our evaluation objective was to assess the FDIC's implementation of ERM against relevant criteria and best practices. We assessed draft and final policies, procedures, and documentation developed as of July 31, 2019, against relevant criteria and best practices such as OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (July 2016) (OMB Circular A-123); the *Chief Financial Officers Council and the Performance Improvement Council Playbook: Enterprise Risk Management for the Federal Government* (July 2016) (CFO Playbook on ERM); and Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management - Integrating with Strategy and Performance* (June 2017) (COSO ERM Framework 2017). The FDIC has taken the position that it embraces the spirit of OMB Circular A-123, even if not required to follow it. The FDIC's implementation of ERM is also informed by the CFO Playbook on ERM and the COSO ERM Framework 2017. From this guidance, we assessed the FDIC against the best practices that, in our professional judgment, aligned with the structure of the Agency and the FDIC's decision to use the OC as its RMC. We assessed the FDIC's actions to implement ERM, including how well the FDIC incorporated ERM processes and communication efforts into the Agency as a whole.

We conducted this evaluation in accordance with Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation*. We engaged the professional services firm of Cotton & Company LLP (C&C) to conduct fieldwork for this evaluation. We also consulted with C&C in preparing this evaluation report. We conducted this evaluation from January to July 2019. We performed our work at the FDIC's offices at Virginia Square in Arlington, Virginia, and Washington, DC. Appendix 1 of this report includes additional details about our objective, scope, and methodology.

BACKGROUND

According to the COSO ERM Framework 2017, ERM integrates the "culture, practices and capabilities" of the organization. According to the CFO Playbook on ERM, the integration of ERM into government management practices allows risks across the enterprise to be "considered and prioritized" as part of "operations support, program management, budget decisions and strategic planning."

In 2016, in an effort to modernize existing agency risk management efforts across the Federal Government, the OMB updated its Circular A-123 on ERM. The revised OMB Circular A-123 required agencies to "implement an ERM capability coordinated with strategic planning and … internal control processes."

OMB Circular A-123 describes documents and concepts that are key to implementing ERM, including the risk appetite, risk tolerance, risk inventory (or risk register), and risk profile. Table 1 includes a description of these documents and concepts:

Table 1: Key ERM Documents and Concepts

Document or Concept	Description
Risk Appetite	Risk an organization is willing to accept in pursuit of its mission.
Risk Tolerance	The acceptable level of variance in performance relative to the achievement of objectives.
Risk Inventory or Risk Register	A list of the risks facing the agency.
Risk Profile	A prioritized inventory of significant risks identified and assessed by an agency through its risk assessment process.

Source: OMB Circular A-123 (July 2016)

OMB Circular A-123 states that the concepts of risk appetite and risk tolerance are essential to achieving effective ERM and determining risk responses. Agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise risk profile. To help develop the risk profile for the agency, the CFO Playbook on ERM suggests that agencies may want to adopt a risk register or risk inventory.[1] After completing the risk register or risk inventory, agencies should examine the risks and include the most significant risks in their risk profile.

The FDIC has taken the position that it embraces the spirit of OMB Circular A-123, even if not required to follow it. The FDIC's implementation of ERM is also informed by the CFO Playbook on ERM and the COSO ERM Framework 2017. The CFO Playbook on ERM provides guidance to help agencies meet the requirements of OMB Circular A-123, and the COSO ERM Framework 2017 provides an ERM Framework for boards and management of organizations. This guidance provides agencies with flexibility to implement ERM in a manner that fits the agency. According to the CFO Playbook, "nothing…should be considered prescriptive…It is not intended to set the standard for audit or other compliance reviews."

[1] OMB Circular A-123 and the CFO Playbook on ERM use the term "risk register." However, the FDIC ERM program refers to the list of risks affecting the FDIC as the risk inventory.

History of ERM at the FDIC

Over the past 15 years, the FDIC has made several attempts at implementing ERM. In 2004, the FDIC initiated the Office of Enterprise Risk Management (OERM) and charged it with administering ERM. At that time, however, ERM at the FDIC was, by design, limited to internal FDIC operations, while external risk management was the responsibility of other Divisions and Offices throughout the FDIC.

2007 OIG Audit Report

In 2007, the OIG issued a report entitled, The FDIC's Internal Risk Management Program, (November 2007), which evaluated the FDIC's overall internal ERM efforts against key concepts and principles of COSO's Enterprise Risk Management Framework (September 2004, in effect at the time) and OMB Circular A-123 (December 2004). This OIG report found that the FDIC had implemented elements of several of the ERM Framework components and had established other internal risk management functions. However, the OIG found that the FDIC's approach to focus solely on internal risks was contrary to COSO's ERM Framework, which defined essential components, suggested common terminology, and provided direction and guidance for ERM. The OIG report noted that ERM should be applied across the enterprise, at every level and unit, and should include an entity-level portfolio view of risk. The report suggested that the FDIC should consider whether the FDIC's "internal and external risk management activities should be integrated."

The report also found that the FDIC should:

- Define and communicate the FDIC's risk appetite and ensure that corporate objectives were aligned with that appetite;
- Implement corporate-wide processes for identifying, assessing, and responding to risks;
- Establish effective channels for OERM to communicate risk information up, down, and across the FDIC;
- Monitor the implementation of ERM;
- Institutionalize how the various committees that aid the FDIC in decision-making interrelate and support ERM;
- Ensure the continuity of risk management efforts as changes in leadership or senior management occur;
- Define the roles of the FDIC Board, Chairman, and Audit Committee in ERM and reconcile the stated role of OERM with actual practice;
- Issue comprehensive procedures and guidance to establish consistent processes, tools, techniques, and models for identifying, assessing and mitigating, and reporting risks; and
- Provide corporate-wide training on ERM.

The report made seven recommendations and two suggestions intended to: (1) address the variances between certain FDIC practices and approaches to ERM and those advocated by the COSO ERM Framework and applicable guidance; and (2) add clarity and structure to ERM. FDIC management agreed to two recommendations to (1) take efforts to more clearly define and communicate the Corporation's risk appetite and ensure that corporate objectives were aligned; and (2) clarify the roles of the Chairman, the Board, and the Audit Committee in relation to ERM. Management also agreed with one suggestion to develop a more comprehensive blueprint to enhance coordination and to document the various committees and groups that contribute to ERM. Management disagreed with the remaining five recommendations and suggestion.[2]

Consultant Report on Risk Management (2010)

In 2010, the FDIC engaged a consulting firm to evaluate its risk management practices and recommend improvements and best practices. The consulting firm identified several gaps in the FDIC's risk management structure in its final report to the FDIC, as shown in Table 2 below.

[2] The OIG has revised its process for reviewing the closure of recommendations, as the OIG now makes the determination as to whether an OIG recommendation is closed or remains unimplemented and reports such information on its website and to Congress. Where the Agency disagrees or non-concurs with an OIG recommendation, it may be reviewed by the Audit Follow-Up Official, in accordance with OMB Circular A-50, *Audit Followup* (September 1982). With respect to this previous OIG report on the FDIC's Internal Risk Management Program (2007), these five recommendations were closed by the FDIC, because despite the OIG's objections, the then-Chairman, who served as the FDIC's Audit Follow-up Official, supported management's response to the recommendations and suggestions.

Table 2: Gaps in the FDIC's Risk Management Structure Identified in 2010

Description of Key Gaps
Scope of Risks
• Not all FDIC risk is properly identified and managed. - No systematic management of new, non traditional risks - Risk requiring cross-divisional management is typically under-managed. • No shared explicit definition of specific FDIC risks versus risks managed as part of ongoing operational role - Notion that "Everything we do at FDIC is risk mitigation" blurs distinction between external risks and resulting FDIC exposure
Organizational Model
• No dedicated and independent roles ensuring all risks are properly managed. - Everyone "manages risk" but no one is a dedicated risk manager. - Existing risk resources report through the divisions. - Resource allocation does not take into account risk impact to FDIC. • Ambiguous risk governance leading to inefficient cross-divisional risk management. - Multiple stakeholders and committees interact on risks but unclear end-to-end coordination and oversight of risks. - Limited responsibility for risk mitigation. • Siloed culture limiting constructive debate and partnership over risks. - Divisions are managed in silos, with limited comfort in sharing information horizontally and vertically.
Risk Management Process
• Existing risk management processes are incomplete and inconsistent. - Processes predominately focused on operational risks with backward looking compliance checks. - Policies and procedures are inconsistent across Divisions and Offices. - No mechanism to share best practices. • Risk management de-prioritized versus day-to-day operations - Focus is on making sure operations react fast and effectively, typically deferring risk management - Lack of forward thinking mindset in risk management
Tools and Infrastructure
• Data is incomplete and lacks the rigor required to ensure appropriate risk management. - Most data is managed independently by divisions and silos, which restricts comprehensive understanding of risk exposure. - New data sets incorporated without clear understanding of content and level of quality - Analyses and projections built off different, independent data sets • Limited development and use of sophisticated risk analysis models and infrastructure - Current infrastructure relies on small numbers of relatively simple tools - Existing risk assessment models do not capture all potential outcomes
Actionable Transparency
• Limited visibility by senior management into entire universe of risks, management activities, and mitigation strategies. - Significant portion of risk reporting is partial, lacks actionable recommendations and is prompted by senior leadership requests

Source: FDIC Consultant Report on *Risk Management* (June 2010)

To address these gaps, the consulting firm made recommendations for the FDIC to:

- Establish a centralized, independent risk management organization headed by a Chief Risk Officer (CRO) reporting directly to the Chairman;
- Establish a small set of risk committees focused on decision-making and overseen by an Enterprise Risk Committee (ERC);
- Require the Chairman and Board of Directors to provide risk management oversight; and
- Develop comprehensive policies and guidelines to govern day-to-day risk management.

The consulting firm also noted credentials and qualifications for the CRO, which included (1) managerial experience over large groups; (2) a strong understanding of the FDIC's operations and the full scope of risks to the FDIC; (3) familiarity with sophisticated risk modeling; (4) knowledge of ERM principles; and (5) being well respected across the organization. To staff the central risk function, the consulting firm recommended a staff of approximately 30-50 employees to supplement the existing risk-related positions at the FDIC.

The Establishment of the Office of Corporate Risk Management in 2011

In response to the consulting firm's recommendations, the then-Chairman appointed a Risk Steering Committee to evaluate the alternatives presented and recommend an organizational structure for risk management within the FDIC. The Risk Steering Committee recommended to the FDIC Board (1) the establishment of a new organizational entity, an Office of Corporate Risk Management (OCRM) headed by a CRO; (2) revision to the corporate Bylaws to designate the CRO as an officer of the FDIC; and (3) development of an organizational plan by the CRO for the operation of the new OCRM for review and approval by the Board.

According to the memorandum to the Board, these changes proposed by the Risk Steering Committee were intended to provide an independent organization within the FDIC that would review internal and external risks with a system-wide perspective; facilitate transparency and sharing of information regarding existing, emerging, and potential risks; and further instill risk governance as part of the FDIC's culture. The FDIC Board approved the recommended changes.

In December 2011, the FDIC created the Office of Corporate Risk Management (OCRM), which started with a core staff of 15 consisting of the CRO, a Deputy CRO, an administrative assistant and 12 professional staff. The CRO reported directly to the Board on key material risks facing the FDIC at least quarterly. OCRM also

developed an inventory of risks facing the agency.[3] An Enterprise Risk Committee (ERC) was established to address internal and external risks facing the FDIC, and was to be the focal point for the coordination of risk management.

The Establishment of the Risk Management and Internal Controls Branch in 2017

In May 2016, the CRO retired, and only five ERM Program staff remained as of September 2017.[4] In September 2017, the FDIC assigned ERM responsibilities to a new office by combining OCRM with the Corporate Management Control Branch within the Division of Finance (DOF) to form a newly constituted Risk Management and Internal Controls Branch (RMIC). The FDIC placed the position of CRO under DOF as a Deputy Director. The FDIC also replaced the ERC with the Operating Committee (OC) as the focal point for the coordination of risk management at the FDIC. The CRO role was no longer designated as an Officer of the FDIC in the FDIC Bylaws. A new Deputy Director of DOF and CRO was appointed in March 2018. The CRO now reports to the Chief Financial Officer and provides briefings to the Chairman on key material risks facing the FDIC.

Current Status of ERM at the FDIC

Since the establishment of RMIC, the FDIC has made progress toward implementing ERM in compliance with government-wide guidance and best practices. In particular, based on interviews with FDIC Division leaders, Divisions are supportive of RMIC's efforts to collaborate and communicate on ERM efforts. According to an FDIC Board member, the current location of the CRO allows for engagement with the Divisions and puts the CRO in a stronger position to carry out the role.

As of December 31, 2019, RMIC had completed or was in the process of completing several key items recommended in both OMB Circular A-123 and by the COSO ERM Framework 2017. RMIC completed a risk appetite statement that was communicated Agency-wide by the Chairman in May 2019. It includes the overall enterprise risk appetite statements for internal and external risks, risks organized into specific categories, risk appetite levels with associated definitions, and risk appetite levels per category. RMIC also completed a risk inventory and risk profile in October and December of 2019, respectively. In addition, RMIC developed example risk

[3] With the establishment of OCRM, OERM was repositioned as a new branch, Corporate Management Control (CMC), in the Division of Finance (DOF). CMC was responsible for managing internal controls and operational risks.
[4] The FDIC initiated a review of OCRM and concluded in the September 2017 memorandum to the Board that ERM efforts under OCRM were not integrated with the rest of the risk management framework at the FDIC. The September 2017 memorandum proposed that OCRM's responsibilities and staff be realigned and integrated with the branch in DOF that had existing responsibility for financial reporting and internal control. The goal was to align the outcomes of ERM activities with the FDIC's annual corporate planning and budget process, which resided in DOF.

tolerances and continues to discuss risk tolerances with the Divisions and Offices.[5] RMIC also developed a training course on ERM for FDIC personnel.
RMIC also revised FDIC Directive 4010.3, and finalized and published the Enterprise Risk Management Standard Operating Procedure (SOP). The CRO has also increased staffing resources in the ERM section to 5 employees and believes the unit is now adequately staffed. RMIC also tracks ERM implementation progress through an internal scorecard that lists specific tasks to be accomplished for the year with an anticipated due date. The scorecard was updated for 2020. Additionally, the FDIC established a performance goal to enhance the FDIC's Enterprise Risk Management program to identify and mitigate risks to key operations across the FDIC.

EVALUATION RESULTS

We found that the FDIC needs to establish a clear governance structure, and clearly define authorities, roles, and responsibilities for ERM. Specifically, we found that:

- The FDIC did not establish clear ERM oversight authorities, roles, and responsibilities for the OC; and
- The FDIC did not clearly define the roles, responsibilities, and processes of the committees and groups involved in ERM.

Unclear Oversight Authorities, Roles, and Responsibilities for the Operating Committee

We found that the FDIC has not established clear ERM oversight authorities, roles, and responsibilities for the OC. The FDIC has designated the OC as the FDIC's RMC and the oversight body for ERM. Given this designation by the FDIC, we would expect the OC to serve the responsibilities of an RMC as outlined in OMB Circular A-123 and the CFO Playbook on ERM. However, we found that the FDIC did not articulate in its policies and procedures how the OC, as the FDIC's designated RMC, performs the following responsibilities:

- Oversight of the establishment of the FDIC's risk profile;
- Oversight of the assessment of risks;
- Oversight of the development of risk responses; and
- Final determinations of the approaches and actions to address the risks in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may

[5] We did not evaluate the risk inventory or the risk profile because they had not yet been completed as of the end of our fieldwork in July 2019. We also did not evaluate the risk tolerances, because the risk inventory and risk profile were still in progress at the completion of our evaluation.

> be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

Having well-defined authorities, roles, and responsibilities for the OC will help the FDIC ensure that ERM is fully integrated into the Agency. If ERM is not fully integrated into the Agency, risks may not be properly identified, assessed, and mitigated. Additionally, having an effective OC helps ensure that risks are considered at the enterprise level by senior officials responsible for program operations and mission support. If risks are not considered by officials with the appropriate knowledge and experience, the FDIC may not prioritize and address the risks that have significant impact on the Agency and the banking sector.

Responsibilities of the Operating Committee

OMB Circular A-123 and the CFO Playbook on ERM suggest four distinct responsibilities of an RMC. Three of those responsibilities are provided in OMB Circular A-123. Specifically, according to OMB Circular A-123, to provide governance for the risk management function, agencies may use an RMC to (1) oversee the establishment of the Agency's risk profile, (2) oversee the regular assessment of risks, and (3) oversee the development of appropriate risk responses. The fourth responsibility of the RMC is provided in the CFO Playbook. Specifically, the CFO Playbook suggests that the RMC, or the agency head, should make the final determinations of the approaches and actions to address the risks in the FDIC's risk profile. To do so, the RMC should have deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

The CFO Playbook on ERM states that:

> [A]fter agency senior leadership have completed their review of the draft agency risk profile, it should be forwarded to the RMC or equivalent for deliberative discussion and consideration around additional actions (proposed risk response) that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite …The RMC or the agency head, as appropriate, should make the final determinations relating to appropriate management approaches and proposed actions based on the agency's risk appetite and tolerance levels.

While OMB Circular A-123 and the CFO Playbook on ERM guidance above are not prescriptive, they are recommended as best practices.

OMB Circular A-123, the CFO Playbook, and the COSO ERM Framework 2017 provide guidance regarding who should serve on the RMC and the importance of

defining roles, responsibilities, and authorities for the RMC. The GAO Publication entitled Standards for Internal Control in the Federal Government (September 2014) (GAO Green Book) explains the importance of an oversight body making oversight decisions so that the entity achieves its objectives.

OMB Circular A-123 states that an effective RMC includes senior officials for program operations and mission-support functions "to help ensure those risks are identified which have the most significant impact on the mission outcomes of the Agency." The CFO Playbook on ERM highlights the importance of defining roles, responsibilities, and ownership of ERM, internal controls, and performance management functions for an effective governance structure. The COSO ERM Framework 2017 also states that "clearly defining authority is important, as it empowers people to act as needed in a given role but also puts limits on authority." Finally, the GAO Green Book provides that "an oversight body oversees the entity's operations; provides constructive criticism to management; and where appropriate, makes oversight decisions so that the entity achieves its objectives in alignment with the entity's integrity and ethical values."

Having the appropriate officials serve on the RMC with defined roles, responsibilities, and authorities is important to ensure the RMC is able to accomplish the four distinct responsibilities described above.

The Resolution of the FDIC Board of Directors (September 2017) defined the OC as the "focal point" for the coordination of risk management at the FDIC. The FDIC further designated the OC as the FDIC's RMC and the oversight body for ERM. Given this designation, we would expect the OC to serve the four distinct responsibilities as outlined in OMB Circular A-123 and the CFO Playbook on ERM, including the (1) oversight of the establishment of the Agency's risk profile; (2) oversight of the regular assessment of risks; (3) oversight of the development of appropriate risk responses; and (4) the final determinations of the approaches and actions to address the risks in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

Charter and Operating Documents Do Not Reflect OC Roles and Responsibilities

The oversight authorities, roles, and responsibilities of the FDIC's OC are not clear. Specifically, the FDIC did not articulate in its policies and procedures how the OC would perform the four distinct responsibilities described above.

The OC Charter, FDIC Directive 4010.3, and SOP define the OC's authorities, roles, and responsibilities, but only at a high level. For example:

- According to the OC Charter (March 22, 2018), the purpose of the OC is to "provide an inter-divisional/office forum for communication, coordination, issue escalation and consensus building." OC members may utilize the committee "as a tool for achieving individual goals such as inter-divisional information sharing … and achieving management consensus."[6] The OC Charter states, however, that the OC is not a decision-making body.

  Moreover, one Division Director stated that OC discussions are strictly for informational purposes. Decisions remain at the Division level. RMIC similarly confirmed that the OC is not a decision-making body and that risk responses and mitigation strategies are handled at the Division level. This current practice at the FDIC is not consistent with the concept of Risk Management on an enterprise level presented in the CFO Playbook on ERM.

  Additionally, the FDIC did not articulate in its policies and procedures how the OC would engage in deliberative discussions regarding the risks facing the FDIC; or consider additional actions to reduce the residual risk based on the risk appetite and tolerance to address the risks in the risk profile. If risk responses for items in the risk profile are determined by the Divisions, it is not possible for the FDIC to ensure that the risks are considered at the enterprise level. Further, the OC cannot ensure that its approaches and actions reduce the residual risk at the enterprise level.

  Moreover, according to the SOP, the OC approves the risk profile on an annual basis. Given that the Committee does not have decision-making authority and does not have procedures for reaching consensus, the FDIC cannot show how the OC accomplishes its responsibility or resolves disputes.

- ERM is one of many subjects that can be brought to the OC. Given the number of OC responsibilities beyond ERM, it is unclear how the OC distinguishes its responsibilities, authority, time, and resources over ERM from other subjects. Therefore, it is unclear how the OC ensures sufficient time and resources are devoted to ERM. According to the OC Charter, "subjects that may be brought to the OC are of a cross-divisional nature. Such subjects include, but are not limited to, FDIC goals and objectives, ERM, general management issues, information technology (IT), physical and IT security, human resources, and facilities management."

- FDIC Directive 4010.3 and the SOP state that the OC is comprised of Division/Office Directors and Deputies to the Chairman who meet periodically

[6] The OC Charter does not clearly articulate what is intended by achieving "individual goals" as part of Enterprise Risk Management.

to address cross-cutting issues, share information about risks, resolve issues, determine next steps, and provide direction. It is unclear, however, how RMIC and Division/Office responsibilities align with respect to the OC. According to the FDIC SOP, Divisions and Offices, in coordination with RMIC, identify and validate an inventory of risks annually; update and validate the risk profile quarterly; perform regular risk assessments; and develop risk responses. However, according to RMIC, in practice, after risks are placed on the risk inventory, they can be raised to the OC for discussion through various methods such as by the Division Directors, the CRO presenting risks from the risk profile, or the FDIC's various risk committees. The OC's feedback may be considered by the responsible Division/Office or Committee when determining how the risk will be managed. This practice, however, is not formalized in the SOP.

While these high-level descriptions support that many different types of issues are discussed by the OC, they do not explain when and how the OC performs the responsibilities laid out in Directive 4010.3 and the SOP such as making ERM oversight decisions, resolving issues, determining next steps, and providing direction. As a result, as the CFO Playbook on ERM warns, there is a risk that the OC will quickly become an empty forum for discussion rather than a source of value in addressing major risks.

Because the OC's oversight authorities, roles, and responsibilities as the FDIC's designated RMC for ERM are unclear, the FDIC did not demonstrate how or if the OC provides (1) oversight of the establishment of the risk profile; (2) oversight of the regular assessment of risks; (3) oversight of the development of risk responses; and (4) final determinations of the approaches and actions based on the risk appetite and tolerance levels to address risks included in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

An effective RMC has an enterprise-wide view of the agency because it is comprised of senior officials for program operations and mission-support functions. Having the RMC make the final determinations of the approaches and actions to address risks included in FDIC's risk profile helps to ensure that risks are identified that have significant impact on the mission outcomes of the Agency and the banking sector. This also ensures mitigation strategies are prioritized and overseen at the enterprise level.

We recommend that the FDIC:

(1) Define, document, and implement the authorities, roles, and responsibilities of the Operating Committee as the RMC, including:
    a) Oversight of the establishment of the Agency's risk profile;
    b) Oversight of the regular assessment of risks;
    c) Oversight of the development of appropriate risk responses; and
    d) Final determinations of the approaches and actions to address the risks in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

In implementing this recommendation, we would expect the FDIC to explain in detail how the Operating Committee will accomplish these roles and responsibilities, including how it will reach consensus, make decisions, and ensure that the Agency prioritizes and addresses the enterprise risks that have significant impact on the Agency and the banking sector.

The FDIC Did Not Clearly Define Roles, Responsibilities, and Processes for Enterprise Risk Management

Effective implementation of ERM requires responsibility for managing risks at all levels of an organization. However, since ERM is not fully implemented at the FDIC, ERM roles, responsibilities, and processes are not fully defined and functioning. Pertaining to the Board, the FDIC did not (1) ensure the Board endorses the risk appetite statement as suggested by the COSO ERM Framework 2017; (2) ensure effective ERM communications to the Board; and (3) ensure that the Board understands its role with respect to ERM at the FDIC.

With regard to the risk committees, the FDIC did not develop procedures to specify how risk committee activities are to be accomplished or how they interface with other ERM processes. We also found that the FDIC did not require documentation of risk committee meetings. Finally, the ERM processes for RMIC, Divisions, and Offices were only broadly defined and did not provide sufficient details or instructions.

Until the FDIC defines these roles, responsibilities, and processes, ERM will not be integrated and consistently applied throughout the Agency and its culture. As a result, employees may not understand how to execute ERM activities and, therefore, risks may not be properly identified and managed.

Roles and Responsibilities of the Board

According to the COSO ERM Framework 2017:

> Effective communication between the board of directors and management is critical for organizations to achieve the strategy and business objectives and to seize opportunities within the business environment. Communicating about risk starts by defining risk responsibilities clearly: who needs to know what and when they need to act. Organizations should examine their governance structure to ensure that responsibilities are clearly allocated and defined at the board and management levels and that the structure supports the desired risk dialogue. The board's responsibility is to provide oversight and ensure the appropriate measures are in place so that management can identify, assess, prioritize, and respond to risk.

According to the COSO ERM Framework 2017, "Management and the board of directors choose a risk appetite with an informed understanding of the trade-offs involved." It also states "Risk appetite is communicated by management, endorsed by the board, and disseminated throughout the entity."

During our evaluation, we found that (1) the Board was not involved in endorsing the risk appetite statement as suggested by the COSO ERM Framework 2017; (2) the FDIC did not provide the same level of information regarding ERM to each Board member; and (3) Board members had different perspectives on the role of the Board in implementing ERM.

In May 2019, the FDIC's risk appetite statement was finalized and communicated by the Chairman without the Board's endorsement. During our evaluation, a Board member explained that the member had limited information on ERM as there had been no formal briefings by the CRO to the Board. Additionally, this Board member had only received a draft of the FDIC's risk appetite statement and had not been briefed on the risk appetite statement before it was finalized. The FDIC provided the Board member the final Risk appetite statement in June 2019. In contrast, another Board member stated that the member was briefed regularly by the CRO on ERM.

Further, one Board member indicated the member had expected that the Board would have a role in ERM implementation. Whereas, another Board member stated that the member's involvement in risk discussions had been project-specific, and expressed that this member did not have a strong opinion regarding the Board's role in implementing ERM. This confusion among Board members occurred because the role of the Board in ERM was unclear. FDIC Directive 4010.3 and the SOP do not define the roles, responsibilities, or communication protocols of the Board within

ERM. According to the Resolution of the Board of Directors (September 2017), the CRO reports to the Chairman quarterly, but the Board can request reports. Additionally, according to the Chairman, the CRO informs the Board of ERM activities through semiannual briefings to the Audit Committee. The CRO also provides quarterly ERM updates to the Chairman, who can make the determination whether ERM issues should be raised to the full Board. However, briefings to the Audit Committee are not the same as briefings to the Board since the Audit Committee does not include the FDIC Chairman nor all of the FDIC's Board members, and the Audit Committee includes a member who is not on the FDIC Board. This prevents the Board members from receiving consistent information on ERM to further the Board's understanding of the risks facing the FDIC.

The FDIC should clearly articulate the role of its Board with respect to ERM. Without doing so, the FDIC cannot ensure that the Board will understand and be able to fulfill its ERM oversight responsibilities. As a result, the Board may not provide the necessary oversight to ensure the appropriate measures are in place so that management can identify, assess, prioritize, and respond to risk.

We recommend that the FDIC:

(2) Define the roles and responsibilities of the Board with respect to ERM, including its role in endorsing the risk appetite statement.

(3) Develop and implement ERM communication protocols to the Board.

Roles, Responsibilities, and ERM Processes of FDIC Risk Committees

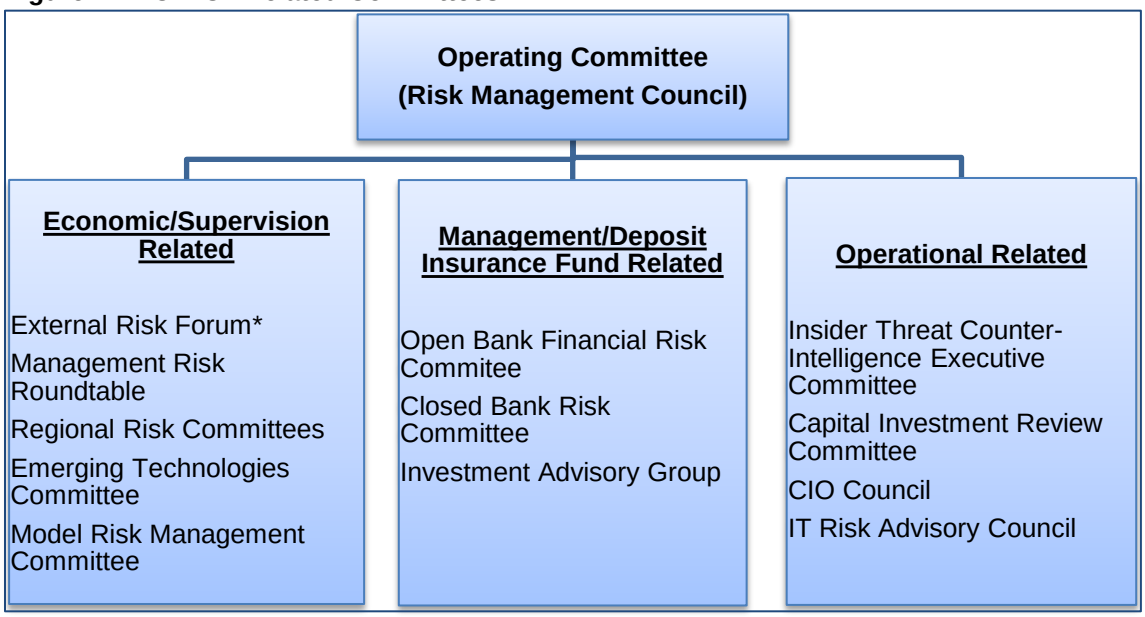
According to the COSO ERM Framework 2017, "Regardless of the particular management committee structure established, it is common to clearly state the authority of the committee … and the specific responsibilities and operating principles... Clearly defining authority is important, as it empowers people to act as needed in a given role but also puts limits on authority."

The GAO Green Book states:

> Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

The ERM SOP references 13 various committees within the FDIC that address significant internal and external risks facing the FDIC (The Figure below lists the FDIC's risk-related committees in place during our evaluation).[7] As noted earlier, the OC serves as the RMC for ERM and was designated by the Board as the "focal point" for the coordination of risk management at FDIC. Given the importance of the OC's role in ERM, we discussed the role of the OC earlier in this report. The other risk-related committees address specific areas of risk such as economic, supervision, management, and operational risks.

Figure: FDIC Risk-Related Committees



Source: FDIC ERM Standard Operating Procedure (May 2019)

**Note: As of August 2019, the External Risk Forum was disbanded and its responsibilities were assumed by the Operating Committee.*

The FDIC, however, did not demonstrate how the various risk committees and their activities are to be accomplished or how they are to interface with other ERM processes, including RMIC and the OC. The FDIC SOP does not provide guidance and does not specify the appropriate level of coordination. It states that "committee meetings provide forums for the identification, discussion, analysis, and elevation of risks." While the CRO may develop additional mechanisms for identifying risks, the SOP does not provide any further details on the risk committee activities.

For example, according to RMIC, risks can be raised by the committees and placed on the risk inventory. However, the SOP does not document a process for how risks raised by the committees are placed on the inventory and by whom.

[7] We did not evaluate these committees or assess their activities. Rather, we obtained an understanding of the general purpose and membership of the various committees.

As a result, FDIC staff may be confused as to whether the Divisions and Office Directors or the Committee chairs have the responsibility for placing risks on the risk inventory. Without clear procedures regarding the role of each committee and how they integrate with ERM, the FDIC cannot be sure that all risks are being identified and placed on the risk inventory.

During our evaluation, the FDIC was not able to provide meeting minutes of the OC and certain committees,[8] as they were not maintained. According to the GAO Green Book, the FDIC should design its internal controls by "establishing and communicating the who, what, when, where, and why of internal control execution to personnel."

Without meeting minutes for the OC, there is no record to support that the committees have identified, discussed, analyzed, and elevated risks. While the other risk committees produce summary reports, these reports may not fully capture the "who, what, when, where, and why" of the decisions discussed in the meetings. Meeting minutes can help the FDIC provide a more complete historical record of "organizational knowledge" and communicate such knowledge to FDIC personnel, auditors, and other stakeholders. The OC began keeping meeting minutes as of September 2019.

We recommend that the FDIC:

(4) Define the roles and responsibilities of each committee in relation to ERM.

(5) Develop and implement procedures on how the risk committees interface with other ERM processes.

(6) Record meeting minutes of the OC and risk committees.

ERM Processes for FDIC Divisions, Offices, and RMIC

According to the GAO Green Book*:*

> Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part

[8] These committees include the Management Risk Roundtable, and Regional Risk Committees.

> of the risk assessment component, management identifies the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities to fulfill defined responsibilities and address identified risk responses.

Per the FDIC's SOP, the implementation of ERM is organized based on the GAO's six essential elements of ERM implementation.[9] GAO's six essential elements of ERM implementation are: (1) Align ERM process to goals and objectives; (2) Identify Risks; (3) Assess risks; (4) Select risk response; (5) Monitor risks; and (6) Communicate and report on risks. Implementation requires a joint effort by RMIC and the individual Divisions and Offices.

While the FDIC SOP describes the tasks for RMIC and other Divisions and Offices with respect to the six essential elements of ERM implementation, it does not outline the procedures necessary to effectively carry out the tasks. The SOP also does not describe what documents are involved in the process, or who has the responsibility to carry out the action(s) within RMIC and the specific Divisions and Offices throughout all six elements. For example, the SOP assigns the Division and Office the tasks of identifying and documenting risk mitigations in a SharePoint site and scoring risks in the inventory. However, there are no related procedures for Divisions and Offices.

Additionally, the SOP references an appendix that provides additional guidance on how to assign a risk score, impact rating, and likelihood rating to risk inventory items. However, the SOP does not outline the seniority of personnel that should be involved in the risk assessment process. The SOP also notes that RMIC will "conduct risk monitoring activities that complement and integrate with Division and Office monitoring activities." However, the SOP does not describe the procedures to accomplish these activities or how results will be tracked.

The ERM SOP broadly defines the ERM program; however, it does not provide sufficient details or instructions as to how FDIC personnel should execute their job functions and roles as part of the ERM program. The broad definitions in the SOP may result in a lack of employee knowledge and inconsistent practices among the multiple Divisions and Offices. Without detailed procedures, Divisions and Offices may not properly identify risks and carry out effective risk mitigation strategies.

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

We recommend that the FDIC:

(7) Develop and implement procedures pertaining to how the Divisions, Offices, and RMIC should execute their particular job functions related to ERM.

In implementing this recommendation, we would expect the FDIC to articulate how risks across the enterprise will be considered and prioritized as part of operations support, program management, resource allocations, budget decisions, and strategic planning.

Integrating ERM with a Strong Governance Structure

According to the CFO Playbook on ERM, ERM should be built around a governance framework supported by senior levels of the organization and integrated into the management of the organization and eventually into its culture. The CFO Playbook on ERM also states that:

> Strong leadership at the top of the organization, including active participation in oversight, is extremely important for achieving success in an ERM program … A strong ERM governance structure helps agency leaders make risk-informed decisions about resource allocation, policy, and operations. As an agency develops its risk governance structure, it is important that it promotes communication and consultation with stakeholders.

ERM is not fully implemented at the FDIC, and, therefore, proper execution of program activities, roles, and responsibilities has yet to take place. Without a clear governance structure over ERM, the FDIC cannot ensure that ERM will fully mature and be integrated into the agency and its culture. Integrating ERM leads to improved decision-making and enhanced performance.

For example, in June 2019, the Chairman announced a reorganization of certain critical functions of the FDIC. The reorganization merged teams from across the FDIC that work on large, complex financial institutions into a new Division of Complex Institution Supervision & Resolution. While the Chairman discussed the reorganization with some members of her leadership team, RMIC, the CRO, and the OC were not consulted or involved in the risk assessment process related to this decision. As a result, there is no assurance that the risks related to the reorganization were considered at the enterprise level by senior officials responsible for program operations and mission-support functions. This demonstrates that ERM has not been integrated into the FDIC processes and its culture. If ERM is not fully matured and integrated into the Agency, there is a risk that the FDIC may not develop a comprehensive portfolio view of risk that would allow the FDIC to make

efficient and effective decisions related to strategic planning, resource allocation, policy, and operations.

We recommend that the FDIC:

(8) Define, document, and implement procedures to ensure that enterprise risks are evaluated using ERM before enterprise-wide decisions are made.

In implementing this recommendation, we would expect the FDIC to describe how information about major risks will flow both up and down the organization and across its organizational structures to improve the quality of decision-making.

Conclusion

Several findings we identified during our evaluation were similar to the findings identified in prior reports, such as the 2007 OIG audit report and the 2010 consultant report. We recognize that the FDIC has made progress in implementing ERM since the establishment of RMIC. However, the FDIC needs to implement the recommendations in this report to establish clear ERM authorities, roles, and responsibilities for the Operating Committee in its role as the Risk Management Council. Further, the FDIC needs to clearly define the roles, responsibilities, and processes of the other committees and groups involved in ERM. Doing so will help ensure that ERM is effectively integrated into the FDIC's culture and that the full range of risks across the enterprise are considered and prioritized as part of its strategic planning, program management, resource allocations, budget decisions, and operations support. The FDIC should continue to mature its ERM program and ensure that a proper governance structure is in place to address the risks facing the FDIC.

FDIC COMMENTS AND OIG EVALUATION

On June 9, 2020, the Deputy Director and Chief Risk Officer of the FDIC's Division of Finance, Risk Management and Internal Controls, on behalf of the Agency, provided a written response to a draft of this report (FDIC Response), which is presented in its entirety in Appendix 3. We reviewed and considered the comments in the FDIC Response.

As discussed in more detail below, the FDIC concurred with five and non-concurred with three of the eight recommendations made in this report. In its response, the FDIC cited program accomplishments achieved in 2019 and noted that it will continue to mature and refine the ERM program, integrate the program into the

FDIC's strategic planning and budget processes, socialize the ERM program at FDIC regional offices, and conduct risk reviews of select FDIC program areas.

The FDIC noted several areas of concerns with our draft report which are addressed below.

OIG's Use of ERM Guidance and Best Practices

The FDIC noted that the OIG evaluated the FDIC's ERM program against relevant criteria and best practices, but also emphasized that the FDIC is not legally obligated to comply with OMB Circular A-123. The FDIC seems to miss the point here. The FDIC should strive to achieve an optimal ERM program based on industry standards, best practices, and recommendations from experts and consultants rather than focusing on their legal obligation to comply or not. Our recommendations provide significant opportunities to improve the FDIC's ERM program. In accordance with the IG Act, the OIG makes recommendations to promote economy, efficiency, and effectiveness in the administration of the FDIC's programs and operations. The OIG's mission extends beyond ensuring mere compliance with laws, regulations, and policies that the agency is required to follow. The FDIC OIG seeks to encourage improvements and efficiencies at the FDIC.

In addition, other experts have identified similar concerns with the FDIC's ERM program. For this particular evaluation, we were assisted by Cotton & Company (C&C) who has assessed the ERM programs of other Federal agencies. The accountants at C&C are experienced and trained in the area of Enterprise Risk Management, and they provided expertise and benchmarking against other Federal agencies in order to enhance our evaluation. C&C fully supported our findings and recommendations.

Our evaluation findings are also consistent with those previously identified in the Consultant's Report on Risk Management in 2010. For example, the consultant noted concerns about the FDIC continuing to manage risks in silos. The consultant noted that multiple stakeholders and committees interacted on risks but the end-to-end coordination and oversight of risks was unclear. The consultant recommended that the FDIC establish a small set of risk committees focused on decision-making and overseen by an Enterprise Risk Committee.

We also note that the FDIC and Federal Financial Institutions Examination Council expect Banks to develop an integrated approach for enterprise-wide risk management to facilitate effective risk identification, measurement, mitigation, monitoring and reporting of risk. The FDIC reviews these programs as part of its bank examinations.

As a result, we believe that the FDIC should be held to high standards of ERM best practices. We do not believe that the FDIC has achieved its full potential in implementing ERM practices, and our recommendations provide significant opportunities to improve the FDIC's ERM program.

Fragmented, Decentralized Approach to Enterprise Risk Management

The FDIC expressed the view in its Response that "it is important that Divisions and Offices own their risks and make risk mitigation decisions, including decisions about appropriate risk responses." However, as noted in our evaluation report, ERM seeks to understand the combined impact of internal and external risks, in an integrated fashion, as a portfolio across the organization, rather than managing risks only within silos. It also helps leaders understand the interrelationships among multiple risks in their agency across the enterprise, and how they present challenges and opportunities when examined as a whole. In addition, ERM can facilitate the proper prioritization of risks and the agency's actions to address them.
If risk responses for items in the Risk Profile are determined by each separate division rather than the OC, these important principles of ERM cannot be fully upheld. Placing ownership of enterprise risks at the Division and Office level and fostering a "decentralized culture of risk identification and mitigation" perpetuates the siloed approach to ERM that best practices do not condone. Our expert accountants, C&C, concur with the OIG's findings and recommendations and they are consistent with the determinations and conclusions reached by the Consultants who reviewed the FDIC operations in 2010, as well.

Role of the Operating Committee

The FDIC chose to use a Risk Management Council (RMC) for its ERM program. The FDIC designated its Operating Committee (OC) as its RMC and the "focal point" for the coordination of risk management. Based on the FDIC's response, it appears the FDIC has chosen not to give the OC the roles and responsibilities of an RMC identified in best practices and has not described an alternative action that will meet the intent of the best practices described below.

The FDIC's Response noted that "the OIG and FDIC have differing views of the OC's appropriate role as the FDIC's RMC." The OIG's view, however, is consistent with the best practices cited by OMB and the CFO Council, the principles of which the FDIC claims its program reflects. The manner in which we describe the role of the OC as the RMC in our evaluation report comes directly from those sources.

We identified these best practices based upon the fact that the FDIC itself determined that an RMC structure was the appropriate structure for the FDIC. It appears, however, that the FDIC has chosen to adopt only the title of the RMC for its OC and has given it a very limited, high-level, and cursory oversight role with no real

impact and authority over risk mitigation and risk response at the enterprise level. According to the FDIC, the OC serves as a "forum for collaborating on specific risks and proposing possible risk mitigation proposals or strategies." As a result, the FDIC has chosen not to follow the best practices related to how an RMC should operate.

The FDIC Response asserted that the OIG believes that "the OC should be the primary deliberative body within the FDIC that determines specific risk response actions for enterprise risks." However, it is not just the OIG who believes this should be the case. As noted in our report, the FDIC Board of Directors designated the OC as the "focal point" for the coordination of risk management at the FDIC. Further, OMB Circular A-123 and the CFO Playbook on ERM suggest that the OC, as the FDIC's RMC, should provide oversight of the establishment of the risk profile, oversight of the assessment of risks and the development of risk responses, and should make the final determinations of the approaches and actions to address the risks included in the FDIC's risk profile. Additionally, as mentioned above, a more centralized ERM process was also supported by C&C and the Consultant from 2010 in their assessments of the FDIC's ERM program. Our findings and recommendations do not and are not intended to limit or constrain decision-making by the Chairman or the FDIC Board. Nevertheless, the OC should make the final determinations on the most important risks facing the agency--those risks included in the FDIC's Risk Profile. If the FDIC does not plan to use the OC in this manner, it should document an alternative process that clearly explains how the final determinations on the most significant and cross-cutting enterprise risks will be made. Indeed, the input and determinations by the OC can be helpful for the Chairman and the FDIC Board as it guides and directs the agency.

Although the FDIC claimed that its current ERM framework allows for "appropriate collaboration while providing necessary agility and flexibility to actively identify and mitigate enterprise risks," it provided no support for such a proposition and has not described how risks will be considered and addressed at the enterprise level. The FDIC also stated that it has "processes in place for deliberating and deciding specific risk-response actions that occur outside of OC meetings that meet the intent of ERM best practices guidance." However, once again, the FDIC did not offer corroboration or an explanation as to how these processes would support its views. Without this information, we see significant potential risk in such processes that occur outside of OC meetings where deliberations and decisions on risk responses are made, as they do not allow for accountability and transparency in the process.

The OC members collectively have the requisite knowledge and experience to prioritize and address the risks that impact the agency. As the focal point for the coordination of risk management at the FDIC, assigning such a role to the OC should not impair agility and flexibility or constrain the decision-making and actions of the Chairman and the FDIC Board, as the FDIC Response suggests. The OC

functioning as the RMC should not supplant or replace effective collaboration and decision-making, but rather it should supplement and enhance the information received by the Chairman and the FDIC Board in making decisions. The Chairman and the Board may benefit from the input, determinations, and opinions of the OC members when making decisions and taking actions.

The FDIC noted in its Response that the CFO Playbook on ERM suggests that the RMC or Agency Head should "be involved in" the final determinations and appropriate risk responses. However, the CFO Playbook on ERM states that the RMC or agency head, as appropriate, should "make the final determinations" on the risks in the risk profile, not just be involved in them. As the Chairman and the FDIC Board of Directors delegated responsibility for risk management to the OC, making the final determinations on risk responses for the risks in the FDIC's risk profile is a role that is fit for the OC. The FDIC response suggests agreement with this point stating that the Deputies to the Chairman and Division Directors, who are also OC members, routinely make such determinations.

Importantly, there is one main difference between the FDIC's view and the OIG's conclusion. That is, the OIG contends that the authorities, roles, and responsibilities should be clear and the final determinations should be made by these individuals in their capacity as an OC member at an OC meeting where ERM is the primary focus of the discussion (rather than in their other roles as Deputies or Division Directors). The process explained by the FDIC as "actively discussed" in "multiple forums" is unclear and does not ensure that there will be deliberative discussions with an ERM focus amongst the officials (all OC members) responsible for programs operations and mission support across the FDIC. If the FDIC does not plan to have the OC make the final determinations on the risks in the risk profile, it should document an alternative approach for how such determinations will be made.

Finally, the FDIC response stated that the OIG "would expect the OC … to make all 'final determinations' on risk responses." We are not expecting that. Instead, we are expecting that while Divisions and Offices can identify and assess risks and determine the appropriate risk responses for their individual Divisions, the OC should be making the final determinations on the approaches and actions for the enterprise, the FDIC as a whole. As explained in our evaluation report and above, this approach is a best practice, because the OC, as the RMC, is comprised of those officials with enterprise-level perspectives on the FDIC's program operations and mission support. The expert accountants at C&C concur with the OIG's findings and recommendations in this regard.

CISR Reorganization

The FDIC stated that the reorganization of CISR "was an important mitigation effort to address concerns regarding existing risks related to potential duplication of effort, lack of coordination, and information sharing, among other things, caused by the distribution of complex financial institution-related staff and responsibilities across multiple Divisions." We acknowledge and understand the FDIC's position. Given the impact of the reorganization on numerous risks in the Risk Profile, it is clear that this decision had enterprise-wide impacts and that evaluating the enterprise-level risks was important.

This view also was supported and recognized by the FDIC when it included "CISR Integration" on its October 2019 Risk Inventory to reflect the risk associated with integrating CISR's expanded responsibilities and personnel. Having the risk on the Risk Inventory will allow RMIC and the CRO to consider it in developing the Risk Profile, which the OC, as the RMC, oversees. This is what our finding suggests should have occurred before the reorganization was finalized in June 2019.

We are not disagreeing with the decision to create CISR. We note, however, that the responsible ERM parties – including RMIC, the CRO, and the OC as the RMC -- were not involved. On September 18, 2019, we met with representatives from RMIC, and confirmed that the OC, CRO, and RMIC had not been involved in the identification of risks regarding the reorganization of CISR, nor had these entities been involved in management's approaches to addressing the risks or its decision-making processes. In addition, the OC was not consulted -- as a Committee -- regarding the final determinations of the approaches and actions to address the risks, thus there was little transparency or accountability for such decisions. The FDIC included "CISR integration" as a risk in its October 2019 Risk Inventory.

This example of RMIC, the CRO, and the OC not being involved in the creation of CISR was discussed with RMIC and the CRO and was included in our discussion draft. The FDIC did not raise any concerns with this example at our exit conference and did not provide any comments on this section of the report when it submitted technical comments in response to the discussion draft report. Therefore, given the numerous prior opportunities to raise such concerns, it is perplexing and troubling to see staunch disagreement in the FDIC Response at this late stage of our evaluation.

Pursuant to the FDIC's SOP on ERM, RMIC and the CRO work with the Divisions and Offices to identify and assess risks. In this case, however, RMIC and the CRO were not involved. Additionally, for such an important cross-divisional reorganization cascading across the FDIC and clearly related to the most significant risks facing the FDIC (as later demonstrated by the issuance of the Risk Profile), the OC, as the

focal point for the coordination of risk management at the FDIC should also have been involved.

It is important to note that although many of the OC members were consulted during the process, it was in their role as a Division head and not in their capacity as an OC member. As we noted earlier, there is a difference between consulting in the role as a Division leader and considering the interests and equities of the Division, as distinct from discussing a risk at the OC with the other members where the primary focus is on the "enterprise," the FDIC as a whole. Leaders wear different hats at different times. To ensure the proper consideration of enterprise risks, it is important for leaders to have deliberative discussions focused specifically on the risks facing the enterprise. Furthermore, while it is not clear which senior leaders were included in the CISR reorganization decision, based on the FDIC's Response, it does not appear the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Division of Information Technology (DIT), the Office of the Ombudsman, and the Office of Legislative Affairs, which are all members of the OC, were involved in the CISR reorganization and the discussion of risks. It would have been important for the CIO, CISO, and DIT to be involved to address any Information Technology (IT) or IT security-related enterprise risks impacted by the reorganization. Additionally, the Office of the Ombudsman could have weighed in on any enterprise risks related to complaints from the banking industry or general public. Finally, the Office of Legislative Affairs could have weighed in on any enterprise risks related to Congressional interests or concerns related to the reorganization.

The FDIC claimed that "the decision-making process that led to the CISR reorganization proposal was an example of this agility and flexibility leading to a proposal for consideration by the Chairman to actually mitigate multiple enterprise risks." This statement indicates that implementing the OIG's recommendations would somehow limit the agility and flexibility of the FDIC in its decision-making, which we are not suggesting. The FDIC provided no support for how the inclusion of the CRO, RMIC, and the OC would somehow limit or constrain the FDIC's agility and flexibility in its decision- making and consideration of risk.

We are not suggesting that the OC needed to be involved throughout the 10-month process in which this decision was being contemplated. Rather, our finding notes that RMIC, the CRO, and the OC, in its role as the RMC, were not consulted or involved in the risk assessment process related to this decision. As our evaluation report noted, the OC serves a critical role in overseeing ERM and making the final determinations on the most significant risks facing that agency – those risks included in the Risk Profile. As the FDIC acknowledged, this reorganization was directly related to many of the risks identified in its own Risk Profile. Therefore, we are suggesting that the OC should have had the opportunity to provide input and inform the final determination. As noted above, this should not impair agility and flexibility or

constrain the decision-making and actions of the Chairman and the Board. Instead, the OC's involvement should supplement and enhance the information received by the Chairman and the Board in making decisions and allow these parties to benefit from the input and recommendations of the OC members.

FDIC Planned Management Actions in Response to the Report Recommendations

The FDIC's responses to several of our recommendations were both vague and inconsistent. The responses included ambiguous terms and provided little or no support for the FDIC's assertions or propositions. Furthermore, in some cases, the FDIC stated it non-concurred with a recommendation but then acknowledged it would take actions to address the recommendation. A summary of each recommendation and the OIG's disposition follows.

Recommendation 1. Define, document, and implement the authorities, roles, and responsibilities of the Operating Committee as the RMC, including:

a) Oversight of the establishment of the Agency's risk profile;
b) Oversight of the regular assessment of risks;
c) Oversight of the development of appropriate risk responses; and
d) Final determinations of the approaches and actions to address the risks in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

The FDIC non-concurred with Recommendation 1; however, the FDIC did not provide an alternative methodology to address the OIG's finding and recommendation. This recommendation is considered unresolved, and we will seek resolution during the evaluation follow-up process.

As discussed in detail above, the FDIC and OIG have differing views on the appropriate role of the OC as the FDIC's designated RMC. We continue to believe that the FDIC should define, document, and implement the authorities, roles, and responsibilities of the OC, as its designated RMC, in keeping with best practices outlined by OMB Circular A-123 and the CFO Playbook on ERM, and as concurred by other experts in the field.

The last paragraph of the FDIC's response for this recommendation does not appear to be consistent with the non-concurrence determination by the FDIC. The FDIC stated that it is "currently evaluating the OC's role in several Corporate areas, including crisis readiness, information technology governance, and… will consider

whether changes to the OC's role with respect to the ERM program are needed." This statement indicates that the FDIC is still evaluating the role of the OC, which supports that the roles and responsibilities of the Operating Committee may still need to be defined, clarified, and implemented.

In addition, the FDIC stated that it will "assess whether the OC charter and [the] existing ERM SOP need to be updated to better explain the OC's oversight role with respect to ERM." These statements are in conflict with each other and the latter statement appears to indicate concurrence with our recommendation. It appears as though the FDIC is indicating that it will nevertheless take the actions we are recommending.

Recommendation 2. Define the roles and responsibilities of the Board with respect to ERM, including its role in endorsing the Risk Appetite statement.

The FDIC concurred with this recommendation, but the actions planned to address the recommendation are not consistent with the intent of the OIG recommendation. Therefore, this recommendation is considered unresolved, and we will seek resolution during the evaluation follow-up process.

As noted in our report, best practices state that effective communication between the Board of Directors and management is critical for organizations to achieve the strategy and business objectives and to seize opportunities within the business environment. Organizations should ensure responsibilities are clearly allocated and defined at the Board and management levels and the Board's responsibility is to provide oversight and ensure the appropriate measures are in place so that management can identify, assess, prioritize, and respond to risk. As noted in our report, the Board members had different perspectives on the role of the Board in implementing ERM, and one member expected to be briefed directly by management and thought the Board should have a role in implementing ERM.

The FDIC's response, however, stated "the CRO will continue to provide semiannual program briefings to the FDIC's Audit Committee" which is "qualified to perform the ERM oversight functions for the Chairman and the Board." As noted in our report, briefings to the Audit Committee are not the same as communicating with the Board because the Audit Committee does not include the FDIC Chairman nor all of the FDIC's Board members. Given the difference in opinion amongst Board members about their role in ERM, we suggest that this approach be revisited to ensure all Board members concur with the approach. The FDIC is a unique agency in that it has a Board of Directors, so in implementing the best practices, it makes sense for the FDIC to incorporate the best practices relevant to a Board of Directors into its ERM processes.

Recommendation 3. Develop and implement ERM communication protocols to the Board.

The FDIC concurred with this recommendation, but the actions planned to address the recommendation are not consistent with the intent of the OIG recommendation. Therefore, this recommendation is considered unresolved and we will seek resolution during the evaluation follow-up process.

The FDIC stated that the Chief Risk Officer will "report to the Chairperson no less frequently than each quarter on the key material risks facing the FDIC" and that "the Chairman may raise issues presented at these ERM quarterly meetings to the Board." In addition, the CRO "will continue to brief the Audit Committee semiannually on the ERM program and enterprise risks."

Given the concerns mentioned above in regard to Recommendation 2 and the differences of opinion amongst Board members about their role in ERM, we suggest this approach be revisited to ensure all Board members concur.

Recommendation 4. Define the roles and responsibilities of each committee in relation to ERM.

The FDIC concurred with this recommendation and stated it will "document the roles and responsibilities of each committee in relation to ERM in a briefing binder." This recommendation is considered resolved and will remain open pending verification of the corrective action by the OIG during the evaluation follow-up process.

Recommendation 5. Develop and implement procedures on how the risk committees interface with other ERM processes.

The FDIC concurred with this recommendation and stated it "will document how the risk committees interface with ERM in the ERM briefing binder." This recommendation is considered resolved and will remain open pending verification of the corrective action by the OIG during the evaluation follow-up process.

Recommendation 6. Record meeting minutes of the OC and risk committees. The FDIC concurred with this recommendation and stated "these committees will begin maintaining meeting minutes." This recommendation is considered resolved and will remain open pending verification of the corrective action by the OIG during the evaluation follow-up process.

Recommendation 7. Develop and implement procedures pertaining to how the Divisions, Offices, and RMIC should execute their particular job functions related to ERM.

The FDIC non-concurred with Recommendation 7; however, the FDIC's reasoning for its non-concurrence was not clear and the response contained inconsistencies. This recommendation is considered unresolved, and we will seek resolution during the evaluation follow-up process.

During the time of our evaluation, we found that the SOP did not describe the documents involved in the ERM process and identify those responsible for carrying out the actions within RMIC and the Divisions and Offices. For example, we noted the SOP assigns Divisions and Offices the tasks of identifying and documenting risk mitigations in a shared site and scoring risks in the inventory. However, we found that there were no related procedures for Divisions and Offices. The SOP also noted, for example, that RMIC will "conduct risk monitoring activities that complement and integrate with Division and Office monitoring activities." However, the SOP did not describe the procedures to accomplish these activities or how results would be tracked. We also noted that in implementing this recommendation, we would expect the FDIC to articulate how risks across the enterprise will be considered and prioritized as part of operations support, program management, resource allocations, budget decisions, and strategic planning.

The FDIC "believes its existing program guidance is adequate and fully responsive to the intent of the OIG's recommendation," but did not explain how the concerns included in our finding had been addressed. The FDIC stated that "the ERM program is supported by an FDIC directive, a detailed SOP, several job aids, a SharePoint solution with embedded user instructions, documentation on how RMIC performs Risk Reviews, and a two-hour ERM training presentation document." However, the job aids, SharePoint solution with embedded user instructions, documentation on how RMIC performs its Risk Reviews, and the training did not all exist at the time of our evaluation. Therefore, while these documents may be sufficient to address our recommendation, we have not had the opportunity to evaluate these documents to determine if they are responsive.

At the conclusion of the FDIC's response to this recommendation, the FDIC stated that it will "update the ERM SOP to address certain OIG recommendations" and "may also update [the] SOP based on the results of lessons learned and ERM maturity model efforts." The FDIC also stated that it will "develop additional job aids as needed." Accordingly, it appears that the FDIC may have intended to concur with this recommendation and submit the cited information to seek its closure during the evaluation follow-up process.

Recommendation 8. Define, document, and implement procedures to ensure that enterprise risks are evaluated using ERM before enterprise-wide decisions are made.

The FDIC non-concurred with this recommendation. It is considered unresolved, and we will seek resolution during the evaluation follow-up process.

The FDIC agrees "that a strong ERM governance structure helps agency leaders make risk-informed decisions," but expressed its concerns that "implementing this recommendation as written could impair or limit decision-making by the Chairman, Deputies to the Chairman, division and office directors, and other senior managers." The FDIC, however, did not provide any support for such a proposition, nor did it explain how or why implementing our recommendation would have such a purported effect.

As we discussed above, having RMIC, the CRO, and the OC evaluate the enterprise risks before an enterprise-wide decision is made, such as the reorganization of CISR, would help to inform and enhance the decision-making process; not restrict, impair, or limit it. Involving all responsible individuals and committees should benefit the process, not replace it. Additionally, having the OC make the final determinations regarding the approaches and actions to address the most significant risks facing the FDIC does not deprive the FDIC of agility and flexibility. Rather it ensures the committee that collectively maintains the operations and mission-support knowledge across the enterprise is given the opportunity to have deliberative discussions and consider the risks and additional actions that may be required to reduce the risks.

The FDIC acknowledged the integration of CISR as an enterprise risk on its inventory in October 2019.

Objective

The objective of our evaluation was to assess the FDIC's implementation of ERM against relevant criteria and best practices.

We conducted this evaluation from January through July 2019 in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. After the completion of our fieldwork but before December 2019, the FDIC completed its risk inventory, risk profile, began recording OC meeting minutes, and developed an ERM training program. While we acknowledged these activities in our evaluation report, we did not evaluate them because they were not completed as of the end of our fieldwork in July 2019.

Scope and Methodology

The scope of the evaluation included assessing draft and final ERM policies, procedures, and documentation; assessing how well ERM processes and communication efforts were incorporated into the FDIC as a whole; and assessing RMIC's actions taken relative to implementing ERM.

We engaged the professional services firm of Cotton & Company LLP (C&C) to conduct fieldwork for this evaluation. We also consulted with C&C in preparing this evaluation report. We monitored the work of C&C, including providing technical guidance and monitoring of contractor activities to determine that the work of C&C could be reasonably relied upon. To accomplish our objectives, we conducted the following procedures covering the scope of the evaluation.

Gained an understanding of ERM by reviewing and analyzing government-wide guidance, best practices, and reports including:

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016)
- GAO Publication, *Standards for Internal Control in the Federal Government* (GAO-14-704G) (September 2014)
- *Chief Financial Officers Council and the Performance Improvement Council Playbook: Enterprise Risk Management for the Federal Government* (July 2016)
- *COSO Enterprise Risk Management - Integrating with Strategy and Performance* (June 2017)

- GAO Report, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk* (GAO 17-63) (December 2016)

The FDIC has taken the position that it embraces the spirit of OMB Circular A-123, even if not required to follow it. The FDIC's implementation of ERM is also informed by the CFO Playbook on ERM and the COSO ERM Framework 2017. From this guidance, we applied the best practices most applicable to the FDIC based on our professional judgment and knowledge of the FDIC.

- Assessed draft and final policies, procedures, and documentation developed as of July 31, 2019, including:
  - FDIC *Enterprise Risk Management and Internal Control Program* Directive (October 2018)
  - FDIC, Enterprise Risk Management Standard Operating Procedure (May 2019)
  - Charters for FDIC risk committees, including the Operating Committee Charter (March 2018)
  - FDIC, Risk Appetite Statement, May 2019
  - FDIC, Risk Inventory (Draft)
  - FDIC, Risk Profile (Draft)
  - Resolution of the Board of Directors (September 2017)
- Reviewed the following reports:
  - FDIC Consultant Report on Risk Management, June 2010
  - OIG Report, *The FDIC's Internal Risk Management Program*, (FDIC OIG EVAL-08-001), November 2007
  - OIG Report, *The FDIC's Information Security Program- 2019*, (FDIC OIG AUD-20-001) (October 2019)

- Interviewed select members of the FDIC's Board of Directors and Division Directors. We also interviewed personnel from DOF's Risk Management and Internal Controls Branch who had responsibility for administering and implementing ERM. We further interviewed the CROs of two other federal agencies on ERM at their respective agencies to understand their practices.

  We performed our work at the FDIC's offices at Virginia Square in Arlington, Virginia, and Washington, D.C.

Appendix 2 Acronyms and Abbreviations

Board	Board of Directors
C&C	Cotton & Company LLC
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CMC	Corporate Management Control
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
DOF	Division of Finance
ERC	Enterprise Risk Committee
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
GAO	Government Accountability Office
IT	Information Technology
OC	Operating Committee
OCRM	Office of Corporate Risk Management
OERM	Office of Enterprise Risk Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
RMC	Risk Management Council
RMIC	Risk Management and Internal Controls Branch
SOP	Standard Operating Procedure

Federal Deposit Insurance Corporation
3501Fairfax Drive, Arlington, VA 22226

DATE: June 9, 2020

MEMORANDUM TO: Terry L. Gibson
Assistant Inspector General for Program Audits and Evaluations
Office of Inspector General

FROM: E. Marshall Gentry /Signed/
Deputy Director and Chief Risk Officer
Division of Finance, Risk Management and Internal Controls

SUBJECT: Management Response to the OIG Draft Report, *The FDIC's Implementation of Enterprise Risk Management* (Assignment No. 2019-001)

The FDIC appreciates the opportunity to comment on the Office of Inspector General's (OIG) draft evaluation report titled, *The FDIC's Implementation of Enterprise Risk Management*, issued on May 19, 2020. This memorandum includes a brief discussion of enterprise risk management (ERM) program achievements, several areas of concerns that we have with the draft report, and our planned actions to address the report recommendations.

ERM Program Achievements and Maturity Efforts

The FDIC is fundamentally a risk management agency. Risk management occurs at multiple levels throughout the organization. For example, the Division of Insurance and Research (DIR) monitors and analyzes emerging risks to the financial industry and economy, while the Division of Risk Management Supervision (RMS) conducts safety and soundness bank examinations. The FDIC ERM program aims to integrate existing risk management practices across functional lines, promote agile decision-making through better flow of information, improve resource deployment, and enhance resilience throughout the Corporation.

The FDIC reorganized ERM responsibilities within the Division of Finance's Risk Management and Internal Controls (RMIC) Branch in September 2017, hired the Chief Risk Officer (CRO) in April 2018, and constituted the ERM team in 2019. Noteworthy program accomplishments during 2019 include:

- Confirmation and distribution of the FDIC's Risk Appetite statement;
- Confirmation of the FDIC's agency-wide Risk Profile;
- Completion of the initial ERM Risk Inventory;
- Issuance of an ERM directive, standard operating procedure, and job aids;
- Development of a SharePoint solution to track ERM risks and mitigations;
- Development of customizable ERM dashboard reports using Tableau;
- Development and delivery of a recurring ERM training course;
- Performance of risk reviews of select topics and program areas;

- Participation in interagency ERM groups to collaborate and learn about other agencies' ERM programs;
- Participation in a working group to update the Chief Financial Officers Council and the Performance Improvement Council's *Playbook: Enterprise Risk Management for the U.S. Federal Government* (July 2016); and
- Participation in a working group with the Council of the Inspectors General on Integrity and Efficiency (CIGIE)[1] to assist in developing ERM audit guidance for the OIG community.

In 2020, we continue to mature and refine the ERM program, further integrate the program into the FDIC's strategic planning and budget processes, socialize the ERM program at FDIC regional offices, and conduct risk reviews of select FDIC program areas. We are also revisiting the Risk Inventory with FDIC divisions and offices in light of the COVID-19 pandemic.

OIG's Use of ERM Guidance and Best Practices as Required Criteria

The OIG evaluated the FDIC's ERM program against relevant criteria and best practices such as:

- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (July 2016) (Circular A-123);
- the Chief Financial Officers Council and the Performance Improvement Council's *Playbook: Enterprise Risk Management for the U.S. Federal Government* (July 2016) (ERM Playbook); and
- the Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management—Integrating with Strategy and Performance* (June 2017) (COSO ERM Framework).

While the FDIC is not legally obligated to comply with Circular A-123, the FDIC generally implements best practices from OMB, and RMIC uses Circular A-123 to help shape the ERM program. The ERM best practices documents give agencies significant discretion to implement ERM programs in a way that best fits an agency's culture and way of doing business, as follows.

The ERM Playbook states:

- *Nothing in the ERM Playbook should be considered prescriptive and all examples provided should be modified to fit the circumstances, conditions, and structure of each agency (or other government organization). The Playbook is not a standard for audit or other compliance reviews.*

[1] CIGIE is an independent entity established within the executive branch to address integrity, economy, and effectiveness issues that transcend individual government agencies and aid in the establishment of a professional, well-trained and highly skilled workforce in the OIGs.

Circular A-123 states:

- *To provide governance for the risk management function, agencies may use a Risk Management Council (RMC) to oversee the establishment of the Agency's risk profile, regular assessment of risk, and development of appropriate risk response. RMC structures will vary by Agency, and in some cases may be integrated with existing management structures.*

- *Agencies have discretion in terms of the appropriate content and format for their risk profiles.*

The COSO ERM Framework states:

- *Management has many choices in how it will apply enterprise risk management practices, and no one approach is universally better than another. Yet, for any entity, one approach may provide increased benefits versus another or have a greater alignment with the overall management philosophy of the organization.*

- *Keep in mind that the benefits of integrating enterprise risk management practices with strategy-setting and performance management practices will vary by entity. There is no one-size-fits-all approach available for all entities.*

Further, CIGIE issued an audit guide for OIGs to use in assessing agency ERM programs (dated January 2020). CIGIE's guide states:

- *There is no one-size-fits-all approach toward ERM. ERM is an iterative process and each agency operates in a unique environment.*

- *OMB Circular No. A-123 provides agencies with flexibility in how to implement ERM, including the format and content of the agency risk profile.*

Our ERM program reflects principles in Circular A-123, the ERM Playbook, ERM guidance issued by COSO and the International Organization for Standardization (ISO), and "essential" ERM program elements noted in a December 2016 GAO report on ERM. Our ERM program also reflects information we learned through our active participation in an ERM community comprised of more than 50 federal agencies. We actively participate in several ERM associations, working groups, policy groups, and training seminars that are focused on furthering ERM programs and sharing best practices.

As noted in the OIG report, the OIG relied on best practices to support its conclusions. These practices are relevant and instructive, but are not prescriptive and are not required. The FDIC endeavors to build the best ERM program possible and considers all best practices, information in ERM guiding documents, and ERM program feedback from other agencies and entities. We consider all suggestions to improve the ERM program and exercise sound judgment and discretion in choosing which practices to adopt and implement, based on FDIC's unique agency profile and operating environment.

Appropriate Role of the Operating Committee as the FDIC's Risk Management Council

The OIG and FDIC have differing views of the Operating Committee's (OC) appropriate role as the FDIC's RMC. The FDIC views the OC as having an ERM oversight role, including providing a forum for collaborating on specific risks and proposing possible risk mitigation proposals or strategies. The OIG, on the other hand, appears to believe the OC should be the primary deliberative body within the FDIC that determines specific risk response actions for enterprise risks.

Based on the FDIC's structure, management's consideration of ERM best practice guidance, and the importance of promoting agility and flexibility in the decision-making and risk-mitigation process, it is vital that the oversight role performed by the OC not be seen as a constraint on appropriate risk-mitigation actions by the Chairman, the Board, division and office leaders, or other senior managers. Ultimately, the Board and the Chairman are accountable for the direction of the agency. The ERM framework in place at the FDIC continues to evolve, but the principles underlying the current ERM framework allow for appropriate collaboration while providing necessary agility and flexibility to actively identify and mitigate enterprise risks.

The FDIC believes it is important that divisions and offices own their risks and make risk mitigation decisions, including decisions about appropriate risk responses. The OC, in turn, oversees the establishment of the FDIC's risk profile, assessment of risk—especially and including risks that cut across multiple divisions and offices—and development of risk responses, consistent with Circular A-123. The ERM Playbook suggests the RMC or the Agency Head be involved in the final determinations of appropriate risk responses. At the FDIC, deputies to the Chairman and division directors, who are also OC members, routinely make such determinations. Decisions on how best to respond to cross-cutting risks are actively discussed among the impacted divisions and offices and risk mitigation strategies are developed collaboratively in multiple forums and managed by oversight and approval mechanisms appropriate for the topic and scope of the mitigation strategy. Additionally, risk identification and mitigation are a critical part of the annual planning, budget formulation, and goals development processes. The FDIC Board of Directors approves the final budget, and the Chairman, in consultation with the Board, approves the annual FDIC performance goals.

The OIG report concludes that because the FDIC designated the OC as the RMC,[2] the OIG would expect the OC to be responsible for ERM oversight and to make all "final determinations" on risk responses. OIG also concludes that if risk responses for items in the risk profile are determined by the Divisions, it is not possible for the FDIC to ensure that the risks are considered at the enterprise level, and the OC cannot ensure that its approaches and actions reduce the residual risk at the enterprise level. As noted above, we believe the internal processes FDIC has adopted to address enterprise-level risks are functioning well and effectively.

[2] It is important to note Circular A-123 does not even require that an agency create an RMC. Circular A-123 guidance was written to provide agencies with flexibility to create an enterprise risk framework and related procedures that best fits the agency's unique culture, mission, and circumstances.

As discussed earlier, the Playbook states, "Nothing in the ERM Playbook should be considered prescriptive and all examples provided should be modified to fit the circumstances, conditions, and structure of each agency…" Under the FDIC's ERM framework, the OC provides ERM oversight, and we have processes in place for deliberating and deciding specific risk-response actions that occur outside of OC meetings that meet the intent of ERM best practices guidance. Further, we do not agree that "it is not possible" for deputies to the Chairman and division directors to appropriately consider and take action to mitigate enterprise risks. These senior management officials identify and determine responses to enterprise risks routinely and in a manner consistent with the FDIC's overall ERM program and risk appetite. Their decision-making process is subject to oversight by the OC and other internal committees, the CRO, the CFO, deputies to the Chairman, the Chairman, the Audit Committee, and the Board of Directors.

Formulating a culture that is responsive to enterprise risk at the lowest-possible decision-making level, while promoting collaboration on risks that require cross-division responses and senior management visibility are critical components of the current FDIC ERM framework. Centralizing all decision-making at the OC would undermine this framework and the decentralized culture of risk identification and mitigation that the framework seeks to create.

OIG's Description of an FDIC Divisional Reorganization

The OIG report suggests the FDIC has not established a strong governance structure around ERM that is supported by senior leaders. The OIG report offers one example to support its conclusion, the FDIC's July 2019 decision to merge several related functions from across the FDIC to form a new Division of Complex Institution Supervision and Resolution (CISR). The OIG report noted:

> "While the Chairman discussed the reorganization with some members of her leadership team, RMIC, the CRO, and the OC were not consulted or involved in the risk assessment process related to this decision. As a result, there is no assurance the risks related to the reorganization were considered at the enterprise level by senior officials responsible for program operations and mission-support functions."

The OIG concluded this example demonstrated that ERM had not been integrated into FDIC processes and culture. For several reasons, we disagree with this conclusion, and the OIG's description of the decision-making process as inconsistent with the FDIC ERM framework.

First, the reorganization was an important mitigation effort to address concerns regarding existing risks related to potential duplication of effort, lack of coordination, and information sharing, among other things, caused by the distribution of complex financial institution-related staff and responsibilities across multiple divisions. The reorganization reduced risk and helped to address multiple items on our Risk Profile, including risks related to the FDIC's ability to:

- Respond to emerging safety and soundness risks;
- Appropriately tailor regulation and supervision based on institution risk and complexity;

- Effectively handle a large insured depository institution failure or a sudden increase in resolution activity;
- Effectively resolve a systemically important financial institution or central counterparty;
- Effectively coordinate across divisions and share information; and
- Address human capital, employee competency, knowledge management, succession planning, and diversity issues.

Implementing any large reorganization can create challenges, however, and the FDIC added a specific item to its risk inventory, titled "CISR Integration," to reflect the risk associated with integrating CISR's expanded responsibilities and personnel.

CISR was established precisely to strengthen the Corporation's risk management and readiness regarding large and complex institutions—and to remedy gaps caused by a legacy organization structure that split this work into four different operational units. Aligning these related skills and operations within a single division has improved coordination and consistency; simplified organizational structure; consolidated specialized skill sets; fostered a collaborative, interdisciplinary approach to our supervision and resolution functions; and promoted internal and external accountability. This organizational change was specifically designed to ensure that information, resources, and expertise are appropriately shared and readily available in the event of a crisis.

Second, the OIG report does not reflect the extensive level of senior-leader engagement and deliberation involved in the reorganization decision. Discussions on the reorganization began in early September 2018 and continued through June 2019. The CISR reorganization was discussed and contemplated extensively by numerous FDIC leaders, including the Chief of Staff, Chief Operating Officer, Chief Financial Officer (to whom the CRO reports), General Counsel, Chief Human Capital Officer (CHCO), and division directors involved in the reorganization. With the exception of the CHCO, each of these officials are members of the OC. The CRO was aware of the plans and intention to create CISR and could have raised risks if necessary. The final reorganization decision was supported by a comprehensive memorandum from the Chief of Staff to the Chairman detailing the rationale, benefits, and challenges associated with the reorganization.

Third, this was an organizational decision that followed the FDIC's standard process for reorganizations. The FDIC has a Corporate directive, *Reorganization Proposals*, to guide major and minor reorganization efforts that requires involvement by senior leaders such as the Chairman, Chief Operating Officer, Chief Financial Officer, and others. The approval process associated with this process provides an additional oversight and risk mitigation feature.

Contrary to OIG's conclusion that there is "no assurance" that senior officials considered risks related to the reorganization, we believe the cited example actually affirms that the Chairman, her deputies, and division directors are very engaged in risk management and employ a thoughtful and informed decision-making process that considers risk consistent with the FDIC's Risk Appetite statement. This ERM framework is already integrated into the agency and its culture and will continue to develop as the ERM program matures.

As noted previously, the OC provides an important oversight function for ERM at the FDIC and discussions at the OC can help target specific risks and develop important proposed solutions to mitigate risk. Mandating the OC as the primary risk-mitigating structure within the FDIC, however, is inconsistent with the FDIC's operating structure, is not required by ERM best practices, and would deprive the FDIC of needed agility and flexibility in addressing enterprise risks.

The decision-making process that led to the CISR reorganization proposal is a good example of this agility and flexibility leading to a proposal for the consideration of the Chairman to actually mitigate multiple enterprise risks. Far from undermining ERM, the deliberative, cross-division discussions that led to the proposal are an illustration of how ERM principles and goals, properly applied, can lead to strong risk-mitigation actions by the Chairman, and, as necessary, the Board or other FDIC decision-makers.

FDIC Planned Management Actions in Response to the Report Recommendations

The OIG made eight recommendations in its draft report. We have carefully considered each recommendation and our responses reflect our desire to continue building the best ERM program possible, while maintaining program flexibility. Our response to each recommendation follows.

Recommendation 1: Define, document, and implement the authorities, roles, and responsibilities of the Operating Committee as the RMC, including:

a) Oversight of the establishment of the Agency's risk profile;
b) Oversight of the regular assessment of risks;
c) Oversight of the development of appropriate risk responses; and
d) Final determinations of the approaches and actions to address the risks in the FDIC's risk profile. These determinations should be based on deliberative discussion and consideration around additional actions that may be suggested or required to reduce the overall level of residual risk and align to the organization's risk appetite and tolerance levels.

In implementing this recommendation, we would expect the FDIC to explain in detail how the Operating Committee will accomplish these roles and responsibilities, including how it will reach consensus, make decisions, and ensure that the Agency prioritizes and addresses the enterprise risks that have significant impact on the Agency and the banking sector.

Management Decision: Non-concur.

Rationale for Management Decision: We appreciate OIG's observations, and we will consider this recommendation as we continue to mature our ERM program. As noted earlier, this recommendation is tied to ERM best practices related to agency governance that are not requirements for the FDIC; are inconsistent with the FDIC's operating model; and would undermine the culture of collaboration, decentralized decision-making, and agility that the FDIC's ERM framework seeks to create. Further, agencies have flexibility in implementing

these practices. After a review of our current ERM governance and practices, we are comfortable that our current model for identifying and mitigating enterprise risks is effective and consistent with these best practices.

Circular A-123 states that agencies *may* use an RMC to oversee the establishment of the Agency's risk profile, regular assessment of risk, and development of appropriate risk response. Consistent with this guidance, we assigned ERM oversight responsibility to our OC. The CRO briefs the OC on the ERM program and Risk Profile quarterly. While there are certainly robust discussions about enterprise risks at OC meetings, final determinations of approaches and actions to address risks (item (d) in the recommendation from the ERM Playbook) often occur outside of OC meetings. Deputies to the Chairman and division and office directors, who are also OC members, make these determinations routinely following established delegations and approval processes, as well as during the annual planning and budget formulation process. This delegated decision-making approach, informed by collaboration and appropriate enterprise oversight, promotes accountability, agility, and flexibility in mitigating risks, while ensuring appropriate senior-level visibility into risk-mitigation decisions.

We are currently evaluating the OC's role in several Corporate areas, including crisis readiness and information technology governance, and we will consider whether changes to the OC's role with respect to the ERM program are needed. We will also assess whether the OC charter and our existing ERM SOP need to be updated to better explain the OC's oversight role with respect to ERM.

Recommendation 2: Define the roles and responsibilities of the Board with respect to ERM, including its role in endorsing the Risk Appetite statement.

Management Decision: Concur.

Planned Action: The CRO will continue to provide semiannual program briefings to the FDIC's Audit Committee. The FDIC will also include the Risk Appetite statement, as a summary agenda item,[3] at the Board meeting to consider the FDIC's annual budget proposal. RMIC will document this information in the ERM SOP.

As established by the Board, the Audit Committee[4] is uniquely qualified to perform the ERM oversight functions for the Chairman and the Board given its responsibilities, including the review and consideration of OIG and GAO reports, its role in budget oversight and the

[3] Any Board member may ask questions about summary agenda items and the Board officially adopts non-report items on the summary agenda, like the Risk Appetite statement, during the course of a Board meeting.
[4] The FDIC Bylaws, Section 1. Standing or Special Committees, states that "The Board of Directors may from time to time establish such standing or special committees as it shall see fit. Any such committee so established shall perform such duties and exercise such powers as may be directed or delegated by the Board of Directors from time to time. Any such standing or special committee shall periodically report its actions to the Board of Directors at such times as the Board of Directors shall determine."

annual financial statement audits, and its oversight of the Corporation's internal controls and assessment of the sufficiency of the Corporation's internal control structure.

In addition, though the OIG suggests the Audit Committee may be inappropriate because a member of the Audit Committee is not a Board member, it is worth noting that the non-Board member serves on the Committee by designation of the Board upon the recommendation of the Chairman.[5] The Audit Committee is actually the only Standing Committee in the Corporation's history to have more than one Board member as committee members. To the extent that Board membership on a Standing Committee is a component in reflecting the value the Board ascribes to a Standing Committee, that makes the Audit Committee the Standing Committee with the most highly elevated membership status.[6]

The Audit Committee will continue to serve as the primary Board component charged with ERM oversight responsibilities, unless otherwise directed by the Chairman or the Board.

Estimated Completion Date: December 31, 2020.

Recommendation 3: Develop and implement ERM communication protocols to the Board.

Management Decision: Concur.

Planned Action: The FDIC has developed and implemented ERM communication protocols to the Chairman, the Audit Committee, and the Board. These protocols are based on an FDIC Board resolution, dated September 2017, which provides that "the Deputy Director for Risk Management and Internal Controls and Chief Risk Officer shall report to the Chairperson no less frequently than each quarter on the key material risks facing the FDIC, with reports to be provided to the Board upon request." The Chairman may raise issues presented at these ERM quarterly meetings to the Board.

In addition, the CRO will continue to brief the Audit Committee semiannually on the ERM program and enterprise risks. The FDIC will also include the Risk Appetite statement, as a summary agenda item, at the Board meeting to consider the FDIC's annual budget proposal.

RMIC will memorialize this information in the ERM SOP.

Estimated Completion Date: December 31, 2020.

---

[5] In 1996, the Board established the Audit Committee in essentially the same manner it exists today. At that time, the Board determined that the third member of the committee, who would not be a member of the Board, would be a very senior official of the Chairman's office and would require a confirming vote of the Board to be designated as a committee member. The Chairman's designee represents the interests of the Chairman on the committee, and provides a mechanism for direct engagement with the Chairman on matters before the committee.

[6] The application of the Government in the Sunshine Act also effectively limits any Standing Committee's membership to two Board Members, particularly those that must consider sensitive internal or supervisory matters.

Recommendation 4: Define the roles and responsibilities of each committee in relation to ERM.

Management Decision: Concur.

Planned Action: The FDIC will document the roles and responsibilities of each committee in relation to ERM in a briefing binder.

Estimated Completion Date: December 31, 2020.

Recommendation 5: Develop and implement procedures on how the risk committees interface with other ERM processes.

Management Decision: Concur.

Planned Action: The FDIC will document how the risk committees interface with ERM in the ERM briefing binder described in recommendation 4.

Estimated Completion Date: December 31, 2020.

Recommendation 6: Record meeting minutes of the OC and risk committees.

Management Decision: Concur.

Planned Action: The OIG reported that 3 of 13 risk-related committees did not maintain meeting minutes. The three committees were the OC, the Regional Risk Committees, and the Management Risk Roundtable (MRR).

As noted in the OIG report, the OC began keeping minutes in September 2019. We provided OC minutes to the OIG for the September and October 2019 meetings.

The Regional Risk Committees produce a detailed report summarizing semiannual regional and headquarters meetings and make these reports available to all FDIC employees on the FDIC's Risk Analysis Center portal. We consider this detailed report to meet the intent of maintaining meeting minutes. Nevertheless, these committees will begin maintaining meeting minutes, beginning with the next series of meetings, which are scheduled for Fall 2020.

DIR usually publishes MRR meeting presentation documents for FDIC employee access on the FDIC's Risk Analysis Center portal. However, the MRR will also begin maintaining meeting minutes, beginning with the next meeting, which is scheduled for June 2020.

Estimated Completion Date: December 31, 2020.

Recommendation 7: Develop and implement procedures pertaining to how the Divisions, Offices, and RMIC should execute their particular job functions related to ERM.

Management Decision: Non-concur.

Rationale for Management Decision: The FDIC believes its existing program guidance is adequate and fully responsive to the intent of the OIG's recommendation. Specifically, the ERM program is supported by a Corporate directive, a detailed SOP, several job aids, a SharePoint solution with embedded user instructions, documentation on how RMIC performs Risk Reviews, and a two-hour ERM training presentation document. The RMIC website includes links to these documents and other ERM resources.

The ERM SOP describes ERM program components (e.g., Risk Appetite statement, Risk Profile, and Risk Inventory); how the ERM program works; how to identify and rate risks; examples of risk tolerances; and the roles and responsibilities of the CRO, RMIC, the Chairman, the OC, divisions and offices, and other ERM stakeholders. We believe this level of policy, procedure, and program guidance is appropriate.

We will update the ERM SOP to address certain OIG recommendations. We may also update our SOP based on the results of an ERM lessons learned initiative and ERM maturity model efforts. We will also develop additional job aids as needed.

Recommendation 8: Define, document, and implement procedures to ensure that enterprise risks are evaluated using ERM before enterprise-wide decisions are made.

In implementing this recommendation, we would expect the FDIC to describe how information about major risks will flow both up and down the organization and across its organizational structures to improve the quality of decision-making.

Management Decision: Non-concur.

Rationale for Management Decision: We agree that a strong ERM governance structure helps agency leaders make risk-informed decisions; however, we are concerned that implementing this recommendation as written could impair or limit decision-making by the Chairman, Deputies to the Chairman, division and office directors, and other senior managers. An effective ERM program should inform and support effective collaboration and decision-making, not supplant it. Moreover, it is vital that the FDIC's ERM framework not deprive the organization of agility and flexibility in the identification and mitigation of risk through an overly centralized decision-making structure.

As discussed earlier, the OIG report suggested the FDIC had not established a strong governance structure around ERM and cited the 2019 reorganization of FDIC's CISR division as an example that demonstrates that FDIC had not integrated ERM into FDIC processes and culture. The FDIC disagreement with this criticism is detailed earlier in this response.

Still, we acknowledge the potential benefit of enterprise-level decisions consistently receiving ERM input, and note that the CRO and RMIC's inclusion in the various Corporate risk committees and as risk managers for significant system development initiatives provides a forum for discussing and responding to risks. Moreover, the CRO's position within the CFO organization, which conducts critical oversight of FDIC budget development and execution, provides an additional avenue to incorporate ERM principles and lessons learned into FDIC strategic planning and operational decision-making. We will continue to enhance risk communication methods and opportunities as we mature our ERM program.

Appendix 4 Summary of the FDIC's Corrective Actions

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC non-concurred with this recommendation and did not provide an alternative methodology to address the OIG's finding and recommendation. This recommendation is considered unresolved, and we will seek resolution during the evaluation follow-up process.	TBD		No	Open
2	The FDIC concurred with this recommendation, but the actions planned to address the recommendation are not consistent with the intent of the OIG recommendation. Therefore, this recommendation is considered unresolved, and we will seek resolution during the evaluation follow-up process.	TBD	$0	No	Open
3	The FDIC concurred with this recommendation, but the actions planned to address the recommendation are not consistent with the intent of the OIG recommendation. Therefore, this recommendation is considered unresolved, and we will seek resolution during the evaluation follow-up process.	TBD	$0	No	Open
4	The FDIC will document the roles and responsibilities of each committee in relation to ERM in a briefing binder.	December 31, 2020	$0	Yes	Open
5	The FDIC will document how the risk committees interface with ERM in the ERM briefing binder	December 31, 2020	$0	Yes	Open
6	The Regional Risk Committees and Management Risk Roundtable will begin recording and maintaining meeting minutes.	December 31, 2020	$0	Yes	Open
7	The FDIC non-concurred with this recommendation. It is considered unresolved, and we will seek resolution during the evaluation follow-up process.	TBD		No	Open
8	The FDIC non-concurred with this recommendation. It is considered unresolved, and we will seek resolution during the evaluation follow-up process.	TBD		No	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
2. Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.

Federal Deposit Insurance Corporation
Office of Inspector General

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

(703) 562-2035

★★★★★★

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

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