Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program

January 2023 **AUD-23-001**

Audit Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

Executive Summary

Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program

The FDIC oversees a supervision program to ensure that FDIC-regulated financial institutions operate in a safe and sound manner and comply with Federal banking laws and regulations. FDIC examiners conduct examinations of financial institutions to assess their financial condition, management practices and policies, and compliance with applicable laws and regulations. The FDIC also conducts information technology (IT) examinations to evaluate bank management's ability to identify IT and cyber risks and maintain appropriate compensating controls.

In June 2016, the FDIC updated its IT examination procedures and implemented the IT Risk Examination (InTREx) program. The InTREx program utilizes a risk-based approach to assess IT and cyber risks at financial institutions. Based on their analyses and conclusions, examiners assign component and composite ratings to financial institutions according to the Federal Financial Institutions Examination Council's Uniform Rating System for Information Technology (URSIT). The URSIT composite rating is a factor in the examiners' determination of the Management component of a bank's CAMELS (Capital, Asset Quality, Management, Earnings, Liquidity, and Sensitivity to Market Risk) rating.

Our audit objective was to determine whether the FDIC's InTREx program effectively assesses and addresses IT and cyber risks at financial institutions.

Results

We found that the FDIC needs to improve its InTREx program to effectively assess and address IT and cyber risks at financial institutions. Specifically, we found the following weaknesses in the program that limit the ability of examiners to assess and address IT and cyber risks at financial institutions:

- The InTREx program is outdated and does not reflect current Federal guidance and frameworks for three of four InTREx Core Modules;
- The FDIC did not communicate or provide guidance to its examiners after updates were made to the program;
- FDIC examiners did not complete InTREx examination procedures and decision factors required to support examination findings and URSIT ratings;

- The FDIC has not employed a supervisory process to review IT workpapers prior to the completion of the examination in order to ensure that findings are sufficiently supported and accurate;

- The FDIC does not offer training to reinforce InTREx program procedures to promote consistent completion of IT examination procedures and decision factors; and

- The FDIC's examination policy and InTREx procedures were unclear, which led examiners to file IT examinations workpapers in an inconsistent and untimely manner.

Moreover, we found that the FDIC:

- Does not provide guidance to examination staff on reviewing threat information to remain apprised of emerging IT threats and those specific to financial institutions;

- Is not fully utilizing available data and analytic tools to improve the InTREx program and identify emerging IT risks; and

- Has not established goals and performance metrics to measure its progress in implementing the InTREx program.

The weaknesses detailed above collectively demonstrate the need for the FDIC to take actions to ensure that its examiners effectively assess and address IT and cyber risks during IT examinations. Without effective implementation of the InTREx program, significant IT and cyber risks may not be identified by examiners and addressed by financial institutions.

An inaccurate assessment of risks may also affect the FDIC's supervisory strategies and examination planning, and increase the risk that URSIT component and composite ratings may not be accurate. Such inaccuracies, in turn, could affect the CAMELS "Management" component rating and the overall composite rating assigned to financial institutions. These ratings are used to determine the insurance premiums paid by the financial institutions.

Recommendations

The report contains 19 recommendations. The report recommends that the FDIC update the InTREx program consistent with applicable guidance as appropriate; ensure examiners complete the InTREx program procedures as intended; file all

supporting workpapers timely; and review and apply threat information regularly. The report also recommends that the FDIC review IT examinations with identified deficiencies and take corrective actions as necessary, and provide refresher InTREx training to examiners to promote consistent completion of IT examination procedures and decision factors. Further, the report recommends that the FDIC determine if the AlphaRex tool could be used to improve the InTREx program and identify emerging IT risks and trends. Finally, the report recommends that the FDIC develop and implement goals and metrics to assess program effectiveness.

The FDIC concurred with 16 of the 19 recommendations and partially concurred with 3 recommendations. For 14 of the 19 recommendations, the FDIC proposed corrective actions that were sufficient to address the intent of the recommendations, and therefore, we consider these recommendations to be resolved and open pending completion of the corrective actions. The FDIC plans to complete corrective actions for these 14 recommendations by December 31, 2023. For the remaining 5 recommendations, we determined that the FDIC's proposed corrective actions do not fully satisfy the recommendations. As a result, we consider these recommendations to be unresolved as of the publication of this report and will work with the FDIC to reach resolution during the audit follow-up process.

Contents

January 31, 2023

Subject ***Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program***

The Federal Deposit Insurance Corporation (FDIC) plays a critical role in maintaining stability in our Nation's financial system by insuring deposits and examining, supervising, and resolving financial institutions. The FDIC serves as the primary regulator for Federally insured state-chartered banks that are not members of the Federal Reserve System.[1] In its role as a financial regulatory agency, the FDIC performs risk management examinations of financial institutions on a 12- to 18- month basis[2] to promote safe and sound operations at the banks.

The FDIC performs examinations to assess specific risk areas involving Information Technology (IT) at banks. The FDIC has established the Information Technology Risk Examinations (InTREx) program to identify, assess, and validate IT and operations risks in financial institutions, and to ensure that these risks are fully addressed by management. Financial institutions depend on IT to deliver services. A disruption or degradation of systems, or unauthorized alteration of information can affect the financial condition, processes, and risk profile of institutions.

According to the FDIC, OCC and FRB, cyber threats against financial institutions are becoming increasingly sophisticated, organized, and a growing area of concern.[3] Those initiating attacks on financial institutions can utilize multiple attack vectors,

[1] The FDIC, the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC), and the National Credit Union Administration (NCUA) have primary responsibility for regulating insured financial institutions at the Federal level. The FRB regulates state chartered institutions that are members of the Federal Reserve System; the OCC regulates Federally chartered institutions; and the NCUA regulates Federally- and state-chartered credit unions.
[2] The FDIC Rules and Regulations Frequency of Examination provision requires the FDIC "to conduct a full-scope, on-site examination of every insured state nonmember bank and insured State savings association at least once during each 12-month period." 12 C.F.R. § 337.12(a). However, for certain small institutions, the FDIC may conduct a full-scope, on-site examination at least once during each 18-month period. 12 C.F.R. § 337.12(b).
[3] FDIC, *2022 Risk Review*; FRB, *Cybersecurity and Financial System Resilience Report* (Sept 2021); and OCC, *Semiannual Risk Perspective* (Spring 2022).

such as social engineering[4] or vulnerabilities in IT systems and third-party software to conduct malicious cyber activities. A report published by IBM Security found that 22.4 percent of cyber attacks it remediated in 2021 were in the finance and insurance sector, with 70 percent of these attacks targeting banks.[5] In addition, a report from a global digital risk firm found that from January 2018 through September 2021, financial services companies suffered nearly 6,500 breaches that exposed 3.3 million records, including email communications, dates of birth, credit card information, addresses, telephone numbers, and account login credentials.[6] The impact of these threats could destabilize the United States financial system.

Our audit objective was to determine whether the FDIC's InTREx program effectively assesses and addresses IT and cyber risks at financial institutions.

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report provides additional details about our objective, scope, and methodology; Appendix 2 contains a list of acronyms and abbreviations; Appendix 3 contains a summary of our sample testing results; Appendix 4 contains a listing of examiner and non-examiner titles and descriptions; Appendix 5 contains the FDIC's comments on this report; and Appendix 6 provides a summary of the FDIC's corrective actions.

BACKGROUND

In July 2021, the Chairman of the FRB identified cyber risk as one of the greatest threats to financial stability.[7] In addition, in August 2022, the Acting Comptroller of the Currency (OCC) noted increases in the frequency and severity of cyber attacks against financial institutions in recent years and warned that attacks have elevated risks beyond the threat of financial loss, including significantly impacting banks' ability to deliver critical services.[8] The Acting Comptroller also urged financial

[4] According to National Institute of Standards and Technology (NIST), social engineering is the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.
[5] IBM Security, *X-Force Threat Intelligence Index 2022* (February 2022).
[6] Constella Intelligence, *Financial Services Sector Exposure Report* (November 2021).
[7] FRB Chairman, *The Semiannual Monetary Policy Report to the Congress* (July 2021).
[8] Acting Comptroller of the Currency, *Remarks before the Joint Meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council* (August 2022).

institutions to assess the potential impact of cyber incidents on institutions, as well as on the financial system.

According to the Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA),[9] ransomware attacks have become the most visible cyber threat to our nation's networks. A ransomware attack is a malicious activity in which attackers encrypt an organization's data and demand payment to restore access or steal an organization's information and demand payment in return for not disclosing the information to authorities, competitors, or the public. A report by Trend Micro Inc., a global cybersecurity firm, found that the banking industry saw an increase of over 1,300 percent in ransomware attacks in the first half of 2021 as compared to the same period a year earlier.[10] Notably, in May 2021, the Carnegie Endowment for International Peace reported that two ransomware groups demanded ransom from three small banks after posting evidence of stolen customer data belonging to the banks.[11]

In addition to ransomware, banks may face other cyber threats, including:

- **Phishing.** A technique that attempts to acquire sensitive data through a fraudulent solicitation in an email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
- **Denial-of-service.** An attack carried out by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access by legitimate users.
- **Data breaches.** An incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so**.**
- **Supply Chain Attacks.** A threat in which an attacker infiltrates an organization's system through an outside partner or service provider.

[9] CISA is a component within the DHS that leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
[10] Trend Micro Inc., *Attacks from All Angles: 2021 Midyear Cybersecurity Report* (September 2021).
[11] Carnegie Endowment for International Peace and BAE Systems, *Timeline of Cyber Incidents Involving Financial Institutions* (April 2022).

According to the Financial Stability Oversight Council's (FSOC)[12] Annual Report for 2021, cyber incidents at financial institutions have the potential to affect hundreds of millions of Americans, resulting in financial losses of billions of dollars due to disruption of operations, theft, and recovery costs.[13] Cybersecurity is a significant concern for the banking industry because of the industry's use of and reliance on technology, not only in bank operations, but also as an interface with customers.

The FDIC has acknowledged that "[c]ybersecurity has become one of the most critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber attacks"[14] and has aimed to bolster cyber incident reporting. On November 18, 2021, the FDIC (along with the FRB and OCC) promulgated a rule requiring banks to report computer security incidents "no later than 36 hours after the banking organization determines that a notification incident has occurred."[15] This rule establishes a Federal requirement for the prompt reporting of destructive cyber incidents at financial institutions and service providers.

Further heightening IT risks and cyber threats is the rapid adoption of technology by financial institutions. According to the OCC's *Semiannual Risk Perspective (Spring 2022),*[16] banks have expanded their use of advanced technologies, such as person-to-person payments,[17] cloud computing,[18] and blockchain distributed ledgers.[19]

In addition, cyber risks may intensify with increased remote work due to the pandemic. Specifically, the technologies needed for remote work introduce additional means for potential cyber attacks, such as through home networks,

---

[12] The Dodd-Frank Wall Street Reform and Consumer Protection Act created FSOC. FSOC's responsibilities include identifying threats to the financial stability of the United States, promoting market discipline, and responding to emerging risks to the stability of the United States financial system. 12 U.S.C. §§ 5321, 5322(a)(1).
[13] FSOC, *2021 Annual Report* (December 2021).
[14] FDIC, *FDIC 2017 Annual Performance Plan* (January 2017).
[15] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 223 (November 23, 2021).
[16] OCC, *Semiannual Risk Perspective* (Spring 2022).
[17] Person-to-Person Payments technology involves the use of mobile devices and applications (internet or mobile) to transfer funds among individuals.
[18] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
[19] According to the NIST, distributed ledgers, such as blockchains, are tamper-resistant digital records of transactions that, once established, cannot be changed. NIST Internal Report 8202, *Blockchain Technology Overview* (October 2018).

routers, laptops, and devices. These networks and devices are typically managed by the employee, and are outside of the organization's security controls and defenses used to protect against ransomware attacks, data breaches, and other types of cyber threats.

Banks also may suffer cyber attacks through interconnections with third parties that provide banks with services, such as accounting, transaction processing, loan servicing, and human resources. According to the OCC's *Semiannual Risk Perspective (Spring 2019)*,[20] consolidation in the bank technology service provider industry has resulted in fewer entities providing these services. In addition, the interdependency of these networks and technologies supporting critical operations magnifies cyber risks, thus threatening the capabilities to mitigate risks at institutions, as well as in the financial sector as a whole.

> In July 2021, cyber-hackers targeted and exploited the remote software of an IT firm, Kaseya, which provides software to banks. Hackers circumvented Kaseya's authentication controls to upload a malicious code. As a result, the hackers were able to access Kaseya customers' networks and install ransomware to encrypt customer data.

The FDIC's IT Supervision Program

The FDIC implements a supervision program to promote safe and sound operations at FDIC-regulated financial institutions. Pursuant to its authorities under the Federal Deposit Insurance (FDI) Act[21] the FDIC serves as the primary Federal regulator for state-chartered financial institutions that are not members of the Federal Reserve System.

Within the FDIC, the Division of Risk Management Supervision (RMS) has primary responsibility for implementing the supervision program. The supervision program is intended to help ensure that FDIC-supervised financial institutions operate in a safe and sound manner and comply with banking laws and regulations.

RMS conducts risk management examinations of FDIC-supervised financial institutions to assess their overall financial condition, management practices and policies, and compliance with applicable laws and regulations. Risk management examinations are performed on a 12- to 18-month basis as required under section

[20] OCC, *Semiannual Risk Perspective* (Spring 2019).
[21] 12 U.S.C. §1811 *et seq*.

10(d) of the Federal Deposit Insurance Act.[22] Risk management examinations are led by a risk management Examiner-in-Charge (EIC) who is responsible for, among other things, managing the examination and assigning the financial institution a Federal Financial Institutions Examination Council (FFIEC)[23] CAMELS rating.[24] The CAMELS rating is used for evaluating the soundness of financial institutions on a uniform basis and for identifying those institutions requiring special attention. The CAMELS rating is also a key factor in assessing a financial institution's deposit insurance premium.[25]

In addition to risk management examinations, RMS conducts examinations to evaluate IT operations risk management practices. IT examinations are conducted as part of the institution's risk management examination process and the results are incorporated into the Report of Examination (ROE). The FDIC's IT examinations are used to identify areas in which a financial institution is exposed to IT and cyber-related risks and to evaluate bank management's ability to identify these risks and maintain appropriate compensating controls.

IT Risk Examination (InTREx) Program

In June 2016, the FDIC updated its IT examination procedures and adopted the InTREx program to provide a risk-focused examination approach. InTREx was developed in partnership with the FRB and Conference of State Bank Supervisors

[22] 12 U.S.C. § 1820.
[23] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the FRB, the FDIC, the NCUA, the OCC, and the Consumer Financial Protection Bureau, and to make recommendations to promote uniformity in the supervision of financial institutions.
[24] In November 1979, the FFIEC adopted the Uniform Financial Institutions Rating System which requires risk management examiners to evaluate a financial institution's performance in six element areas and ultimately determine an overall composite rating. The six components, represented by the "CAMELS" acronym, include: Capital adequacy, Asset quality, Management, Earnings, Liquidity, and Sensitivity to market risk. Examiners assign each CAMELS component with a rating of 1 through 5, and an overall composite rating of 1 through 5.
[25] In addition to its financial institution supervisory role, the FDIC maintains the Deposit Insurance Fund (DIF), which is used to insure the deposits at banks and resolve failed banks. The DIF is funded by insurance premiums paid by financial institutions and the interest earned on funds invested in U.S. government obligations. A financial institution's insurance premium is risk-based and determined differently based on the bank's size. Small banks (generally, those with less than $10 billion in assets) are assigned an individual rate based on a formula using financial data and CAMELS ratings. Large banks (generally, those with $10 billion or more in assets) are assigned an insurance premium rate based on the CAMELS ratings, financial measures used to measure a bank's ability to withstand asset-related and funding-related stress, and a measure of loss severity that estimates the relative magnitude of potential losses to the FDIC in the event of the bank's failure.

(CSBS) drawing on materials such as the FFIEC IT Examination Handbook,[26] the FFIEC Cybersecurity Assessment Tool (CAT),[27] and the Interagency Guidelines Establishing Information Security Standards.[28] The OCC and NCUA were not part of the process to develop the InTREx program.

The InTREx program utilizes a risk-based approach to assess IT and cyber risks at financial institutions. Specifically, examiners tailor the IT examination's strategy, scoping, and performance of examination procedures to each financial institution based on risks they identify. At the conclusion of an IT examination, examiners are required to assign component and composite ratings according to the FFIEC's Uniform Rating System for Information Technology (URSIT).[29] Specifically, examiners evaluate and assess the institution's ability to identify, measure, monitor, and control IT risks for the functions identified within four URSIT component areas: Audit, Development & Acquisition, Management, and Support & Delivery (see Table 1). Based on this analysis, examiners rate each URSIT component area on a scale from 1 ("strong") through 5 ("critically deficient").

Table 1: URSIT Component Areas

Audit	This rating reflects the adequacy of the organization's overall IT audit program, including the internal and external auditor's abilities to detect and report significant risks to management and the board of directors in a timely manner.

[26] The FFIEC IT Handbook consists of a series of individual IT Booklets which provide the financial regulatory agencies with guidance and examination procedures for assessing IT risks at financial institutions. The FFIEC IT Booklets provide guidance in the following IT areas: (1) Audit; (2) Business Continuity Management; (3) Development and Acquisition; (4) Information Security; (5) Management; (6) Architecture, Infrastructure, and Operations; (7) Outsourcing Technology Services; (8) Retail Payment Systems; (9) Supervision of Technology Service Providers; and (10) Wholesale Payment Systems.
[27] The FFIEC developed the CAT, consistent with the principles of the FFIEC IT Handbook and NIST Cybersecurity Framework, to assist institutions in identifying their IT and cyber risks to determine their cybersecurity preparedness. The FFIEC does not require financial institutions to utilize the CAT.
[28] The Interagency Guidelines (12 CFR Appendix B to Part 364) set forth standards pursuant to the Gramm-Leach-Bliley Act (GLBA), which requires financial regulatory agencies to establish appropriate standards for financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
[29] On December 20, 1996, the FDIC Board of Directors adopted the FFIEC's updated statement of policy entitled "Uniform Financial Institutions Rating System" (UFIRS). The updated UFIRS replaces the 1979 statement of policy and is effective January 1, 1997.

Development & Acquisition	This rating reflects an organization's ability to identify, acquire, install, and maintain appropriate IT solutions. Specifically, the processes and practices for purchasing hardware or software, the development and programming performed by the institution or service provider, and the services from independent vendors or affiliated data centers, or a combination of these activities.
Management	This rating reflects the abilities of the board and management as they apply to all aspects of IT acquisition, development, and operations. Depending on management's practices, this rating may address some or all of the following IT-related risks: strategic planning, quality assurance, project management, risk assessment, infrastructure and architecture, end-user computing, contract administration of third-party service providers, organization and human resources, and regulatory and legal compliance.
Support & Delivery	This rating reflects an organization's ability to provide technology services in a secure environment. It reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information delivery system. Risk management practices should promote effective, safe, and sound IT operations that ensure the continuity of operations and the reliability and availability of data.

Source: FFIEC IT Handbook.

Examiners assign an URSIT composite rating which is based on the overall results of the evaluation and the URSIT component ratings. The URSIT composite rating is used in the determination of the Management component of a CAMELS rating.

InTREx Examination Workflow

The FDIC's InTREx program uses a workflow that consists of three key phases: 1) Pre-examination, 2) Examination, and 3) Reporting and Monitoring.

Pre-examination. During the pre-examination phase, examiners perform steps to identify risk indicators[30] at financial institutions in order to develop the examination's scope. Prior to the start of the examination, examiners send the financial institution an IT Profile, a risk based questionnaire, which is used to assign a complexity level to the institution based on the responses. Financial institutions that are deemed most complex are designated "InTREx Level A", moderately complex "InTREx Level B", and least complex "InTREx Level C." The InTREx Level designation is used to assign the lead examiner-in-charge for IT examinations ("IT EIC").

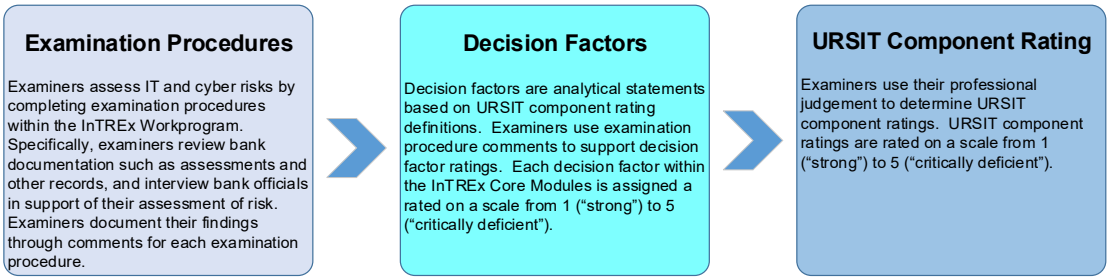
[30] Risk indicators include activities that increase the complexity of IT environments and introduce additional operational risks at financial institutions. For example, a bank that manages its critical processes in-house or provides services to other institutions has a heightened level of risk due to the complexity and heavy reliance on the bank's internal controls for its IT environment.

Once assigned, the IT EIC issues a documentation request to the financial institution called an IT request list. The requested bank documents help to develop the IT examination scope comment.[31] This defines the IT examination's scope and strategy and identifies high-risk areas that the examination team should focus on during the examination.[32]

Examination. During the examination phase, FDIC examiners and staff execute the InTREx Workprogram according to the IT examination scope. The InTREx Workprogram is organized into four InTREx Core Modules that are mapped to the URSIT component areas (Audit, Development & Acquisition, Management, and Support & Delivery).[33] The InTREx Workprogram consists of examination procedures, decision factors, and is used to assign URSIT component ratings for each InTREx Core Module.[34]

See Figure for a description of the InTREx Core Module Workflow.

Figure: InTREx Core Module Workflow



Source: OIG-developed based on FDIC InTREx program procedures.

[31] The IT examination scope comment is provided to the risk management EIC for inclusion in the risk management Pre-examination Memorandum which outlines the risk management examination activities and procedures for the risk management examination.
[32] Examiners may determine the need for expanded or supplemental workprograms to adequately assess risks that are not covered in the InTREx Core Modules. In some cases, the lack of risk indicators may result in limited reviews for certain examination procedures. For example, examiners may not perform procedures to assess source code and programming controls for financial institutions that do not develop or use custom software.
[33] The InTREx Workprogram also includes optional expanded and supplemental examination procedures, used to assess specific IT products or services not covered in the InTREx Core Modules.
[34] In addition to examination procedures and decision factors, examiners are provided control testing procedures to validate the institution's controls and procedures. According to the InTREx procedures, control test procedures should be performed at the discretion of examiners based on the perceived risk in the area under review, and may leverage control testing performed by internal or external auditors.

Examiners are to exercise their discretion in determining the depth of their review[35] but are required to complete all examination procedures and decision factors. Completion of each Core Module is based on the documentation submitted by the financial institution, interviews with key personnel, control testing, and direct observations.

Information Security Standards and Cybersecurity Preparedness Assessments

In addition to determining URSIT component and composite ratings, the InTREx Workprogram is used to determine the financial institution's compliance with the Interagency Guidelines Establishing Information Security Standards ("Interagency Guidelines") and assess their cybersecurity preparedness. The Interagency Guidelines set standards for financial institutions in developing and implementing an information security program to protect customer information from threats. The cybersecurity preparedness assessment determines the bank's implementation of cybersecurity principles and standards set forth in the National Institute of Standards and Technology (NIST) Cybersecurity Framework[36] and the FFIEC CAT.

The examination procedures used to determine compliance with Interagency Guidelines and cybersecurity preparedness[37] are embedded within the InTREx Workprogram examination procedures. The results of the assessments are detailed separately from the URSIT composite and component ratings in the ROE.

Reporting and Monitoring. The ROE contains a summary of the overall condition of the IT function, compliance with Interagency Guidelines, and the financial institution's cybersecurity preparedness. The ROE also contains comments for each URSIT component, as well as the component and composite ratings. If the examination team issues recommendations, management's response and corrective actions are also included in the ROE.

In cases where significant IT issues are identified, the IT comments may warrant inclusion of Matters Requiring Board Attention (MRBA). The FDIC defines an MRBA as "an issue or risk of significant importance that requires board attention." For more

[35] FDIC examiners may expand or limit their work to support examination procedures based upon the level of risk identified during pre-examination or during their review.
[36] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (February 2013) directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for managing and reducing cyber risks to critical infrastructure.
[37] The procedures used to assess a financial institution's cybersecurity preparedness are known as "Baseline Cybersecurity Statement" procedures, discussed in more detail later in our report.

serious concerns, or instances where MRBAs have not been addressed, the FDIC is authorized to take corrective actions, known as enforcement actions, against financial institutions. MRBAs and enforcement actions are tracked and monitored through the Virtual Supervisory Information on the Net (ViSION) application.[38]

InTREx Interagency Committee

The InTREx Interagency Committee is comprised of representatives from the FDIC, FRB, CSBS, and NCUA.[39] The Committee is responsible for overseeing the process to identify and update changes to specific aspects of the InTREx program, such as the IT Profile, IT Profile scoring, and the InTREx Workprogram. The OCC does not participate on the InTREx Interagency Committee.

While the FDIC, FRB, and CSBS continue to oversee the InTREx program collectively, each of these regulatory agencies manages its own IT examination process differently. Specifically, the CSBS coordinates the development of legislative and regulatory policies among the state banking regulatory agencies; however, each state agency is responsible for managing its own respective IT examination policies and procedures. For example, we found that not all state agencies are utilizing the InTREx program, and in some cases, were utilizing a limited version of the InTREx program to conduct their IT examinations.

A survey conducted by the CSBS[40] found that 10 percent of responding state agencies were not utilizing the InTREx program, and that 35 percent (14 of 40) were either using a shortened version of the InTREx workprogram or a combination of both the full and shortened versions.[41] According to RMS officials, the FDIC has an alternating examination schedule with state agencies and occasionally conducts joint examinations.

---

[38] The ViSION application provides automated support for many aspects of financial institution supervision, including application tracking, case management, safety and soundness examination, IT examination, offsite monitoring, large bank analysis, management reporting, workload management, processing, and security.

[39] In 2020, the NCUA initiated a pilot of the InTREx program and joined the InTREx Committee in an observational capacity.

[40] On May 31, 2022, the CSBS conducted a survey of state banking agencies to assess the number of state agencies that are currently utilizing the InTREx program. As of August 16, 2022, 40 state banking agencies have responded.

[41] FDIC examiners must review prior-year ROEs for both FDIC- and state- led examinations in support of examination planning, and may also review supporting workpapers to obtain additional details. Our audit was limited to FDIC led IT examinations and did not assess whether the varying ways in which state agencies implemented their IT examinations impacted the FDIC.

In addition, the FRB uses a "baseline" InTREx Workprogram for non-complex financial institutions that includes a reduced number of examination procedures. FRB officials stated that due to limited resources and time constraints needed to conduct full scope IT examinations, the FRB utilizes a baseline InTREx Workprogram which serves as a streamlined version of the program. According to FRB officials, the baseline InTREx Workprogram includes less than half of the examination procedures in the InTREx Workprogram "while maintaining the themes of the full scope workprogram." In addition, the FRB uses an expanded IT Profile with six additional questions designed to identify the complexity of the bank and risk factors.

IT Examinations at Other Financial Regulatory Agencies

The OCC does not utilize the InTREx program and is not a member of the InTREx Interagency Committee.[42] OCC officials noted that at the time of development, it was their understanding that the program was limited to the supervision of state-chartered banks.[43] FDIC officials stated that participation in the InTREx program was offered to all financial regulatory agencies and InTREx was designed for all financial institutions. After the InTREx program was established, the FDIC offered to make the InTREx program available for the OCC. The OCC continues to use its own IT examination process outlined in its "Bank Supervision Process" booklet within the OCC's Comptroller's Handbook.[44]

For complex midsize and large banks, OCC examination specialists use the FFIEC IT Examination Handbook to guide their assessment, while community bank examiners conduct IT examination procedures outlined in the OCC's "Community Bank Supervision" booklet.[45] The Community Bank Supervision booklet establishes procedures that examiners perform to develop conclusions and assign an URSIT rating. However, as opposed to the FDIC, the OCC only assigns an URSIT composite rating to its community banks.

In July 2020, the NCUA piloted a modified and streamlined version of the InTREx program to examine credit unions. The modifications included removing the IT profile and reducing the number of examination procedures and decision factors. However, in 2021, the NCUA decided to end the InTREx pilot and apply the lessons learned to reinstate and improve its existing IT examination program with the goal of

[42] While the OCC is not a member of the InTREx Interagency Committee, the OCC and the other FFIEC interagency partners do regularly meet to share and collaborate in support of developing uniform reporting systems for Federally supervised financial institutions.
[43] The OCC supervises national banks and Federal savings associations, and Federal branches and associations of foreign banks.
[44] OCC, *Bank Supervision Process*, Version 1.1 (September 2019).
[45] OCC, *Community Bank Supervision*, Version 1.1 (September 2019).

having procedures finalized by the end of 2022. The NCUA continues to participate on the InTREx Interagency Committee as an observing member.

FDIC Roles and Responsibilities

FDIC's Division of Risk Management Supervision is divided into six groups: (i) the Office of the Director; (ii) Operations; (iii) Operational Risk; (iv) Supervision and Policy; (v) Capital Markets; and Accounting Policy; and (vi) Supervision and Policy – Large Banks.[46] The primary responsibilities of the Operational Risk group are to oversee RMS's information technology, cybersecurity, and Bank Secrecy Act[47] examination programs, and to monitor financial crime activities and related risks to the FDIC-supervised institutions.

Within the Operational Risk group is the IT Supervision Branch, which is responsible for identifying and addressing emerging operational and IT risks and supporting the examination process to promote the safety and soundness of financial institutions. Specifically, the IT Supervision Branch core responsibilities include:

- Identifying technological and operational threats, and recommending mitigating strategies;
- Providing oversight for IT examinations, including the InTREx program;
- Delivering cybersecurity and information technology guidance, policy and procedures to internal and external entities; and
- Ensuring examiners are highly trained and effective to support the FDIC's IT examination process.

RMS has six supervisory regional offices: Atlanta, Chicago, Dallas, Kansas City, New York, and San Francisco. Each regional office is led by a Regional Director (RD) who reports to the Director of RMS and the Director of Depositor and Consumer Protection[48]. The primary responsibilities of the regional offices involve assessing risks to the DIF and overseeing the supervisory activities of field offices to mitigate those risks. Field offices, which report to the regional offices, are

[46] The Supervision and Policy – Large Banks group oversees supervisory and monitoring programs for state non-member banks with total assets exceeding $10 billion. In June 2019, the FDIC established the Division of Complex Institution Supervision and Resolution to oversee banks with total assets greater than $100 billion for which the FDIC is not the Federal primary regulator.
[47] The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970, often referred to as the Bank Secrecy Act, established anti-money laundering recordkeeping and reporting requirements for financial institutions.
[48] The Division of Depositor and Consumer Protection has primary responsibility for examining and supervising FDIC-insured institutions for consumer protection.

responsible for conducting various institution examinations. Examiners and examination support staff work in the FDIC field offices.

IT Examination Staffing and Training

IT examinations are conducted by commissioned examiners[49] and specialized IT examination support staff. All commissioned examiners receive training to enable them to lead an InTREx examination at the lowest level of complexity (InTREx Level C). FDIC examiners can obtain additional skills and experience through the FDIC's Intermediate or Advanced IT On-The-Job Training (OJT) programs to become qualified to lead more complex examinations (InTREx Levels B and A, respectively). Risk management examiners who complete these programs are identified by RMS as either Intermediate IT Subject Matter Experts (SME) or Advanced IT SMEs.

The FDIC's IT examination staff also includes a group of personnel who have advanced IT examination knowledge and specialized IT experience called IT examiners. IT examiners serve as the supervisory region's IT experts with responsibility for planning and conducting complex IT examinations.

Additionally, the FDIC has developed two non-examiner IT examination positions—IT Examination Analysts (ITEA) and IT Cyber Analysts (ITCA)—to support IT examinations. See Appendix 4, *Examiner and Non-Examiner Titles and Descriptions*, for additional details on IT examination staff roles and responsibilities.

IT Examination Staffing Risk

As part of the its Enterprise Risk Inventory,[50] the FDIC has identified a risk that it may not be able to maintain a sufficient number of IT SMEs to assess IT risks and implement an effective supervisory strategy. According to personnel data obtained from the FDIC's Division of Administration and RMS, the retirement eligibility for

[49] According to Section 10(b) of the FDI Act, examiners appointed (or commissioned) by the FDIC's Board of Directors have the power to perform examinations on behalf of the Corporation. The process for commissioning examiners involves an intensive training and development process over a multi-year timespan that includes: on-the-job training, formal instructor-led examiner training, and self-directed study. Pre-commissioned examiners must also demonstrate their skills, knowledge, and proficiency by successfully completing examiner benchmarks and a Technical Evaluation. Finally all pre-commissioned examiners must receive a recommendation from the candidate's field supervisor to be promoted to a commissioned examiner.

[50] The FDIC's Chief Risk Officer and Office of Risk Management and Internal Controls maintain the Risk Inventory to capture the enterprise risks identified by the FDIC's Divisions and Offices. FDIC Divisions and Offices have responsibility for keeping the Risk Inventory updated throughout the year, and for conducting an annual, agency-wide validation. The Risk Inventory informs the development of a prioritized list of the most significant risks facing the FDIC, known as the Risk Profile.

Advanced IT SMEs and Intermediate IT SMEs was 31 percent and 18 percent, respectively, for 2022. These retirement eligibility rates increase to 64 percent and 33 percent, respectively, in 2027. These rates far exceed the government-wide retirement eligibility rate, which was 15 percent in 2022 and is 30 percent for 2027. In addition, in 2021 and 2022, the FDIC experienced significant resignations of examiners in training at rates greater than pre-pandemic levels. Without an adequate number of IT SMEs and examination staff, the FDIC may not have the IT expertise needed to identify and assess significant IT risks. In addition, a shortage of IT SMEs could impact the FDIC's ability to conduct IT examinations at the current examination frequency (12- to 18- months) for its most complex financial institutions.

AUDIT RESULTS

We found that the FDIC needs to improve its InTREx program to effectively assess and address IT and cyber risks at financial institutions. Specifically, we found the following weaknesses in the program that limit the ability of examiners to assess and address IT and cyber risks at financial institutions:

- The InTREx program is outdated and does not reflect current Federal guidance and frameworks for three of four InTREx Core Modules;
- The FDIC did not communicate or provide guidance to its examiners after updates were made to the program;
- FDIC examiners did not complete InTREx examination procedures and decision factors required to support examination findings and URSIT ratings;
- The FDIC has not employed a supervisory process to review IT workpapers prior to the completion of the examination in order to ensure that findings are sufficiently supported and accurate;
- The FDIC does not offer training to reinforce InTREx program procedures to promote consistent completion of IT examination procedures and decision factors; and
- The FDIC's examination policy and InTREx procedures were unclear, which led examiners to file IT examinations workpapers in an inconsistent and untimely manner.

Moreover, we found that the FDIC:

- Does not provide guidance to examination staff on reviewing threat information to remain apprised of emerging IT threats and those specific to financial institutions;

- Is not fully utilizing available data and analytic tools to improve the InTREx program and identify emerging IT risks; and

- Has not established goals and performance metrics to measure its progress in implementing the InTREx program.

The weaknesses detailed above collectively demonstrate the need for the FDIC to take additional actions to ensure that its examiners effectively assess and address IT and cyber risks during InTREx examinations. Without the effective implementation of the InTREx program, significant IT and cyber risks may not be identified by examiners and addressed by financial institutions.

Until the FDIC addresses these weaknesses, there is a risk that IT and cyber risks at banks will not be identified or adequately mitigated or addressed. As a result, financial institutions may be more susceptible to cyber attacks and threats. The lack of accurate assessments may also affect the FDIC's supervisory strategies and examination planning. In addition, there is an elevated risk that URSIT component and composite ratings may not be accurate. This, in turn, could impact the CAMELS 'Management' component rating and the overall composite rating assigned to financial institutions, which is used to, among other things, determine the financial institution's deposit insurance premiums.

The FDIC's InTREx Program Is Outdated

GAO Internal Control Standards[51] state that management should periodically review procedures for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. These periodic reviews should consider significant changes, such as personnel, operational processes, or information technology.

The InTREx Interagency Committee is responsible for overseeing the process to identify and update changes to the InTREx program. According to an InTREx Interagency Committee representative, the primary driver for initiating updates to the InTREx program is the issuance of new or revised FFIEC IT Booklets and FFIEC guidance. In addition, the InTREx Interagency Committee Charter charges the

[51] GAO, *Standards for Internal Control in the Federal Government (Internal Control Standards)* (September 2014).

Committee with ensuring the InTREx program "remain[s] current, effective, risk-focused, and aligned with supervisory guidance." However, we found that recent updates to FFIEC IT Booklets and NIST guidance were not incorporated into the InTREx program.

Specifically, we found that the InTREx program had not been updated to address the following FFIEC guidance and updates to two of the FFIEC IT Booklets:

- In August 2021, the FFIEC issued "Authentication and Access to Financial Institution Services and Systems" guidance, which provides risk management principles and practices, and reinforces the need for financial institutions to effectively authenticate users and customers to protect information systems, accounts, and data.

- In November 2019, the FFIEC revised the "Business Continuity Planning" IT booklet. The updated booklet outlines business continuity management principles to address risk related to the availability of critical financial products and services. In addition, the updated booklet places a focus on enterprise-wide approaches that address technology, business operations, testing, and communication strategies critical to the continuity of the business. Further, the booklet identified risks within supply chain management.

- In June 2021, the FFIEC updated the "Operations" IT booklet. The booklet assesses an entity's governance of common risks related to Architecture, Infrastructure, and Operations; enterprise-wide IT architectural planning and design; implementation of virtual and physical infrastructure; and the entity's operational controls. In addition, the FFIEC IT booklet addresses emerging technologies, such as cloud computing, micro-services, artificial intelligence, machine learning, zero trust architecture, and the Internet-of-Things. Further, the booklet incorporates cybersecurity considerations and practices for technology employed at financial institutions.

In addition, the InTREx program was developed in accordance with the NIST *Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework"), version 1.0 dated February 2014. However, NIST has since updated its Cybersecurity Framework in April 2018,[52] and these changes are not reflected in the InTREx program. Specifically, supply chain risk management activities found in the NIST Cybersecurity Framework are not addressed in the InTREx examination procedures. For example, the FDIC does not have procedures that assess the

[52] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (April 2018).

financial institution's processes for identifying, addressing, and managing supply chain risks.

Organizations inherently face supply chain risks when contracting with third parties for goods and services. According to NIST, supply chain risk management is critical to ensuring business resilience as organizations can no longer protect themselves by simply securing their own infrastructures as threat actors intentionally target the suppliers to take advantage of the weakest link. Further, organizations may have reduced visibility, understanding, and control of these risks when their vendors rely on second- and third-tier suppliers and service providers.

In December 2020, Federal agencies experienced a supply chain attack involving the network services provider SolarWinds, Inc, (SolarWinds).[53] Specifically, attackers infiltrated SolarWinds' software supply chain and inserted malicious code that created backdoor access into the product. Once customers installed software updates, attackers gained unauthorized access to the customers' network environments. The National Security Council's Cyber Unified Coordination Group noted that approximately 18,000 public and private sector customers, including Federal agencies and financial institutions, were compromised by this supply chain attack. These risks are heightened in the banking industry as many financial institutions rely on third-party service providers, or vendors, to deliver IT products and services.

In February 2021 and 2022, the OIG identified assessing supply chain risks as a Top Management and Performance Challenge facing the FDIC.[54] Also, in March 2022, the OIG issued an evaluation report[55] on the FDIC's implementation of Supply Chain Risk Management (SCRM). Specifically, we found that the FDIC:

- Had not implemented several objectives to identify, evaluate, and monitor supply chain risks;
- Was not conducting supply chain risk assessments during its procurement process;
- Had not integrated supply chain risks into its Enterprise Risk Management (ERM) processes; and
- Did not properly maintain contract documents.

---

[53] SolarWinds, Inc. is a software development company that offers products and services to assist entities in managing their networks, systems, and information technology infrastructure.
[54] FDIC OIG, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (February 2021); *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (February 2022).
[55] FDIC OIG, *The FDIC's Implementation of Supply Chain Risk Management* (EVAL-22-003) (March 2022).

As a result, we made nine recommendations to improve the FDIC's SCRM program and retention of contract documents. The OIG recommended that the FDIC identify, document, and monitor supply chain risks and conduct supply chain risk assessments of suppliers and vendors. The OIG also recommended that the FDIC's Enterprise Risk Management program articulate the extent and significance of supply chain risks. As of January 2023, six recommendations remain open and unimplemented.

These reports highlight the importance of identifying, evaluating, and mitigating supply chain risks and vulnerabilities that threaten the FDIC's ability to fulfill its mission, goals, and objectives; protect its sensitive and nonpublic information; and maintain the integrity of its operations.

The InTREx Interagency Committee has made one update to the InTREx program since it was established in June 2016. Specifically, the InTREx Interagency Committee updated the IT Profile and Support and Delivery (S&D) Core Module in July 2019, more than 3 years ago. According to an InTREx Interagency Committee representative, the Committee began the process to update the Audit and Management Core Modules in December 2019. However, as of November 2022, nearly 3 years later, these updates had not been completed. RMS officials explained that the delay was due to contributing factors, such as the pandemic and key personnel turnover.

In addition, the InTREx Interagency Committee lacks formal procedures to ensure that changes to the InTREx program are efficient, timely, and measurable. The Committee has not developed any guidance or procedures outside of the InTREx Interagency Committee Charter. Moreover, the Charter only outlines the Committee's responsibilities at a high level and does not require the Committee to establish controls activities. The GAO Internal Control Standards emphasize the importance of policies and procedures as critical components of an effective internal control system. For example, policies and procedures serve as an important control for reducing operational risk associated with changes in staff.

The evolving nature of IT and cyber risks underscores the need for timely updates to examination procedures for the InTREx program. Without an effective process to update the InTREx program, the FDIC cannot ensure that its examiners are applying current IT guidance to assess all significant risks. The lack of an effective process also increases the potential that banks may be operating in IT environments with unidentified and unmanaged risks.

Recommendations

We recommend that the Director, RMS:

1. Update and implement the InTREx program to reflect current IT and cyber risks and guidance.

2. Work with the InTREx Interagency Committee to develop and implement procedures to govern the process to update the InTREx program.

The FDIC Did Not Communicate InTREx Program Changes to FDIC Personnel in a Timely Manner Nor Provide Guidance to Implement the Program Changes

The GAO Internal Control Standards state that "effective information and communication are vital for an entity to achieve its objectives." The Internal Control Standards state that agency management should have appropriate methods to communicate information based on the intended recipients, nature of the information, availability, cost, and legal requirements. In addition, the Internal Control Standards highlight the importance of establishing procedures by stating that "management communicates … procedures so that personnel can implement the control activities for their assigned responsibilities."

In July 2019, the InTREx Interagency Committee updated the IT Profile and S&D Core Module in the InTREx program. Specifically, the Committee reduced the number of questions in the IT Profile from 26 to 13. In addition, the scoring system used to determine the financial institution's complexity level was updated.

The changes to the S&D Core Module introduced 58 new procedures for examiners to indicate when Baseline Cybersecurity Statement procedures were not met. Previously, the Baseline Cybersecurity Statement procedures shared the comment box with examination procedures, which made it difficult to determine whether these steps had been performed. According to the FDIC representative to the InTREx Interagency Committee, by removing the Baseline Cybersecurity Statement procedures from the examination procedures into a separate checklist, management can better ensure that these steps are being properly performed and documented.

However, we found that the FDIC did not communicate these InTREx program changes to its personnel and provide guidance for how to implement the updates. Specifically, these changes were made in July 2019, yet RMS never issued a Regional Director Memorandum (RMS RD Memorandum) or any guidance to inform its examination staff of these InTREx updates. RMS's primary means for communicating its procedural updates and changes to supervisory regions and staff is through the issuance of RMS RD Memorandums.

In addition, we found that RMS RD Memorandum 2016-009, which established the InTREx procedures, had not been updated to include links to the updated IT Profile

and S&D Core Module. After we brought this issue to the attention of RMS IT Supervision Branch officials in March 2021 during the course of our fieldwork, the links to the updated IT Profile and S&D Core Module were subsequently updated in the RMS RD Memorandum 2016-009. However, as of the date of this Report, the FDIC has not issued any additional guidance to examiners nor to financial institutions in order to notify them of the update.

The Charter for the InTREx Interagency Committee requires partner agencies to "post approved changes [to the InTREx program] to their respective internal websites." Specifically, the Charter states that "agencies will issue internal notifications of updated modules consistent with normal agency processes."

According to FDIC officials in the RMS Operational Risk group, the lack of an RMS RD Memorandum was an oversight, and it plans to issue formal notifications for each subsequent update to the InTREx program. While the FDIC did not notify its personnel of these changes, it had uploaded the updated S&D Core Module template to the RMS collaborative platform for examiners and IT examination support staff.

Without communication or guidance related to InTREx program updates, the FDIC cannot ensure that its examiners are implementing the InTREx program effectively and as intended. For example, in 2 of the 10 FDIC bank examinations we reviewed as part of our sample testing,[56] we found that examiners had incorrectly used an outdated IT Profile and S&D Core Module. The two examinations were performed more than 5 months after the IT Profile and S&D Core had been updated, further highlighting the need for effective communication and guidance from the FDIC.

In addition, we found that some FDIC examiner staff were unclear on how to address changes in the updated S&D Core Module. For example, the Baseline Cybersecurity Statements fields were previously embedded in examination procedures but were now separated into a check list. FDIC examiners stated that they were not provided guidance or instructed on how to complete the checklist, or whether it was required.

In 4 of the 10 FDIC examinations reviewed, we found that examiners had identified cybersecurity-related deficiencies but had not included these issues in the corresponding Baseline Cybersecurity Statement fields as required. For example, in one examination, the examiner found deficiencies in the financial institution's patch

[56] See Appendix 3, *IT Examination Sample Testing Summary*, for a summary of our sample testing results.

management program that were described in the individual examination procedures and S&D Core Module summary, but were not reflected in the Baseline Cybersecurity Statement fields as required. As a result, these key deficiencies were not included in the Cybersecurity Preparedness Workpaper[57] and importantly, were similarly not included in the Cybersecurity Preparedness summary comment in the ROE. Therefore, the FDIC cannot ensure that bank management was properly informed of these cyber-related risks.

The FDIC did not adequately communicate changes to the InTREx program or provide guidance to its examiners. As a result, FDIC examiners were not aware of management's expectations in completing the updated S&D Core Module and did not execute the InTREx program as intended. The lack of communication and guidance led to inconsistencies and increased the possibility that FDIC examiners may not have assessed all significant IT and cyber risks at banks. Such risks could lead to inaccurate URSIT ratings by the FDIC examiners.

Recommendations

We recommend that the Director, RMS:

3. Communicate updates to the InTREx program to examiners in a timely manner and prior to implementation.

4. Issue revised or updated guidance to examiners to address InTREx program updates.

Incomplete IT Examination Procedures and Decision Factors by FDIC Examiners Led to Potentially Inaccurate URSIT Ratings

The InTREx program utilizes a risk-based approach that relies on examiners to complete all examination procedures to support decision factor ratings. In addition, FDIC examiners must assess each decision factor, which along with the completed examination procedures, is used to determine the URSIT component ratings. Documentation to support ratings should generally describe key audit decisions, risk-scoping determinations, source documents reviewed, and examination procedures performed.

We found that FDIC examiners did not complete examination procedures and the decision factors needed to support examination findings and URSIT ratings, as

[57] Examiners are required to summarize their cybersecurity assessment and assign a rating in the Cybersecurity Preparedness Workpaper.

required by the InTREx program. Specifically, for 70 percent (7 of the 10) of the IT examinations reviewed, FDIC examiners had not documented the work performed for required procedures:

- For three examinations, FDIC examiners had not input comments for procedures required to assess management's practices on information security program oversight. For example, examiners did not complete procedures to evaluate the financial institution's information security policy and procedures, or those used to assess vendor oversight.

- For three examinations, FDIC examiners had not completed examination procedures to assess operational and security activities, such as monitoring controls or electronic funds transfer oversight in the S&D Core Module.

- In one examination, we found no evidence that FDIC examiners had completed procedures needed to address project management and third-party risk in the Development & Acquisition Core Module. These procedures address the oversight practices and controls of vendors who provide critical services to the institution.

In addition, examiners did not complete each decision factor used to support URSIT ratings.[58] Completed decision factors are used by examiners to facilitate the assignment of component and composite ratings. However, we found that in 40 percent of the IT examinations reviewed (4 of 10 examinations), examiners had not completed all decision factors. For example:

- In three examinations, multiple decision factors were not assessed in the S&D Core Module. Further, in one of the three examinations, all five of the required S&D Core Module decision factors were not completed.

- In one examination, we found two of the four decision factors in the Development & Acquisition Core Module were not completed.

GAO Internal Control Standards state that control activities can be used to ensure that operational processes are complete and accurate. However, we found that the FDIC has not established an effective control process to ensure that examiners complete procedures and decision factors.

[58] Decision factors are assessed on the following scale: "Strong", "Satisfactory", "Less than satisfactory", "Deficient", and "Critically deficient".

Without complete InTREx examination procedures and decision factors, the FDIC has limited assurance that risks are being properly assessed and that URSIT ratings are accurate. For example, for two of the four examinations in which FDIC examiners had not assessed decision factors, a change in an URSIT component rating could have resulted in an overall lower URSIT composite rating:

- In *Examination 1*, the four URSIT component ratings were split between "1" and "2" ratings with an URSIT composite rating of "1." Had the affected URSIT component rating changed from "1" to a "2" (or lower), the shift could potentially have resulted in an URSIT composite rating downgrade.

- In *Examination 2*, we found that three of the URSIT component ratings were rated "2" and the remaining component was rated "3." Had the affected URSIT component rating changed from a "3" to a "4" (or lower), the shift could potentially have resulted in an URSIT composite rating downgrade.

Changes to the URSIT composite rating could also lead to a change in the CAMELS Management component rating, which could affect the overall CAMELS composite rating and, among other things, the financial institution's deposit insurance premiums. This impact is significant, as the CAMELS ratings is used to assess a financial institution's deposit insurance premium to insure depositors' accounts against loss.

Recommendations

We recommend that the Director, RMS:

5. Develop and implement control mechanisms to ensure that examiners complete examination procedures and decision factors.

6. Review the sampled examinations in which examination procedures and decision factors were not completed in order to determine whether or not the ratings are accurate.

7. Take corrective actions to address any inaccuracies identified as a result of the review recommended above.

The FDIC Lacks a Process for the Review of IT Examination Workpapers

As described previously in this report, we found that 7 of 10 IT examinations we sampled had incomplete examination procedures and 4 examinations had decision factors that were not assessed. The FDIC could not demonstrate that its IT EICs nor supervisors had conducted any review of IT examination workpapers prior to the

issuance of the ROE. For example, there was no documentation to support that an FDIC supervisor had reviewed the underlying examination work.

The FDIC's examination policy and InTREx procedures do not establish a process for the review of IT examination workpapers prior to issuance of the ROE. Specifically, the FDIC's examination guidance does not assign responsibility for reviewing workpapers during an IT examination. Instead, the FDIC relies on workpaper reviews conducted by RMS's Internal Control and Review Section (ICRS) and the supervisory regions after the completion of the examination to evaluate its IT examination operations and assess compliance against the FDIC's examination policy and InTREx procedures. Specifically, RMS's ICRS performs reviews on one third of the FDIC's regions (two of six regions) annually. The reviews consist of an evaluation of a sample of 10 IT examinations, judgmentally selected and conducted over a 6-month period. Each supervisory region conducts workpaper reviews at its respective region for a varying number of IT examinations and at varying frequencies (for example, annually, bi-annually).

In addition to being conducted after the completion of the examinations, these reviews are also only completed on a small number of examinations. As a result, an ICRS or supervisory region review would not prevent an ROE with incorrect or unsupported findings from being issued. In addition, we found that both reviews typically assess whether examiners had complied with guidance but not whether the work performed was adequate or whether conclusions were sufficiently supported and accurate.

Moreover, ICRS reviews are not shared with all supervisory regions, further limiting their effectiveness in the FDIC's IT examination process and supervision. For example, we found similar findings in multiple ICRS reports that may have been avoidable if supervisory regions were able to leverage other ICRS reports and take preventive actions. Ultimately, ICRS reviews do not replace the role of a supervisory workpaper review process.

By contrast, FRB's *Examination Manual* establishes a formal workpaper review process for IT examinations that requires workpapers to be reviewed by the EIC or designated senior personnel, and for reviewers to document when their review is completed by signing or initialing each applicable document.[59] According to the *FRB Examination Manual*, these reviews should be performed as soon as practicable after the completion of each work area in case additional work is required. Without formal guidance or a mechanism to document whether reviews of workpapers were

[59] FRB, *Commercial Bank Examination Manual* (May 2021).

completed properly, the FDIC cannot ensure that IT examination findings were sufficiently supported and accurate.

Recommendations

We recommend that the Director, RMS:

8. Update and implement examination policy and InTREx procedures to require that IT examination workpapers be reviewed for adequacy and that workpapers sufficiently support examination conclusions prior to the issuance of the ROE.

9. Share the results of ICRS Regional Reviews with all supervisory regions.

Training to Reinforce InTREx Procedures Needed

The FDIC's IT examiners are required to perform each examination step according to the examination procedures and assess all decision factors in the InTREx Core Modules. These examiners determine the depth of review for each examination procedure according to identified risks. In addition, examiners are responsible for assigning the URSIT component and composite ratings based on their analysis. To help ensure that examiners are adequately prepared to make such discretionary judgments, the FDIC provides a commissioning program and ongoing training opportunities.

According to GAO Internal Control Standards, it is the responsibility of management to establish expectations of competence for key roles to help the organization achieve its objectives. Competence, which is the qualification to carry out assigned responsibilities, is gained largely through professional experience, training, and certifications.

After examiners are commissioned, the FDIC requires examiners to complete two training courses - Information Technology Examination Course (ITEC)[60] and Introduction to Security - and a 90-day IT examination rotation to obtain on-the-job experience. However, once examiners complete these requirements, the FDIC does not provide further training to reinforce InTREx program requirements, such as the completion of all examination procedures and decision factors, or to address updates

[60] ITEC is a comprehensive course that educates examiners on the concepts within each of the InTREx Core Modules and teaches examiners how to develop examination conclusions and assign URSIT ratings.

and changes to the InTREx program. Additional InTREx-related training would help to reduce errors and reinforce InTREx guidance and updates. Such training would be effective for examiners who do not regularly perform IT examinations.

We issued a survey to examiners and IT examination support staff to obtain their feedback on the InTREx program.[61] With respect to training, 42 percent of respondents (116 of 273) identified insufficient training as a material challenge to conducting IT examinations.

According to officials within the RMS Operational Risk group, supervisory regions provide refresher training to examiners who have not used InTREx "for an extended period of time." However, only four of six supervisory regions could provide the materials used for refresher training. In addition, only one of the four supervisory regions reinforced InTREx guidance, such as instructing examiners to complete all examination procedures and decision factors. RMS officials acknowledged the need for consistent InTREx refresher training across all supervisory regions and are in the process of developing these materials.

Without training to reinforce InTREx program guidance and instruct examiners on addressing updated procedures, the FDIC is at risk that examiners will not consistently perform IT examinations as intended. We found that only 1 of 10 IT examinations sampled had been performed consistent with the requirements of InTREx procedures. In other words, 90 percent of IT examinations reviewed did not comply with InTREx procedures. By offering training courses for examiners, the FDIC can improve the consistency, reliability, and results of IT examinations.

Recommendation

We recommend that the Director, RMS:

10. Provide refresher training to reinforce InTREx program procedures, such as the completion of all examination procedures and decision factors, and address updates and changes to the InTREx program.

FDIC Policy and Procedures for Maintaining IT Examination Workpapers Are Unclear

FDIC examiners prepare workpapers to document and describe the work performed during an InTREx examination. Workpapers include details such as the identified IT risks and control weaknesses, documents obtained from banks, and other support

[61] See Appendix I, *Objective, Scope, and Methodology* for survey scope and methodology.

for findings. The FDIC uses the Regional Automated Document Distribution and Imaging system (RADD) to capture, index, distribute and store electronic documents related to its supervision program. FDIC examiners are required to retain all relevant workpapers to support their comments and findings in the RADD system. With respect to IT examinations, workpapers include the IT Profile, IT Profile Validation, InTREx Workprogram, expanded examination procedures, and any supplemental workprograms.

InTREx procedures require "all IT examination workpapers to be scanned and imported into RADD." However, we found that examiners did not always file certain IT examination workpapers used to support findings and URSIT ratings. We reviewed a sample of 10 examinations and found multiple instances in which examiners had not filed IT examination workpapers that supported findings and ratings in RADD:[62]

- For 40 percent of examinations (4 of 10), examiners did not upload the IT Profile and IT Profile Scoring Matrix. The IT Profile Validation workpaper is used to record the financial institution's risk indicators and determine the InTREx complexity. This information is significant to the assignment of resources, including the IT EIC. Should the incorrect IT EIC be assigned, examiners may not have the appropriate knowledge, skills, and experience to assess the IT environment effectively. Further, the IT Profile is a significant tool in scoping of IT examinations to identify risk areas that require additional workprograms or expanded reviews.

- For one examination sampled, examiners did not upload the Interagency Guidelines and Cybersecurity Preparedness Workpapers. Examiners are to summarize the financial institution's compliance Interagency Guidelines and assess the institution's cybersecurity controls in each respective workpaper. These summaries are provided to financial institutions as part of the ROE.

- For one examination sampled, the examiner did not upload any of the InTREx Core Modules, Interagency Guidelines, and Cybersecurity Preparedness workpapers. The InTREx Core Modules include all examination procedures and decision factors used to support the examination findings, conclusions, and ratings. In addition, we noted that these workpapers were missing for at least 10 months after the date of the ROE.

[62] After we brought these deficiencies to the FDIC's attention on July 27, 2021, the identified workpapers were filed in RADD.

The FDIC identified similar issues in prior ICRS Regional Reviews. Specifically, in its Regional Reviews of the Atlanta (2017) and New York (2018) regions, examiners had not filed workpapers in RADD:

- In the Atlanta Regional Review report, ICRS issued a recommendation for the region to strengthen its InTREx program by, among other things, ensuring workpapers are uploaded to RADD. However, this recommendation was not implemented, because in the Atlanta Regional Review report issued in 2021, the ICRS review once again found that examiners had not retained the required examination workpapers in RADD.

- In the New York review, the ICRS report noted that duplicated workpapers were available in different RADD folders, some workpapers were not appropriately labeled, and there were missing workpapers. The report stated that examiners were ultimately able to provide all missing workpapers. The FDIC has not yet conducted a follow-up ICRS review to assess workpaper retention at the New York supervisory region.

The FDIC's examination policy and procedures do not establish roles and responsibilities for maintaining workpapers relating to IT examinations. Specifically, the InTREx procedures do not assign the responsibility of review and oversight of workpapers to the IT EIC. Therefore, the procedures leave responsibility for all workpaper maintenance oversight, including IT examination workpaper maintenance, to the risk management EIC. However, four IT EICs stated it was their responsibility to ensure that all IT examination workpapers were uploaded to RADD. Because the practice for maintaining IT examination workpapers is not consistent with the FDIC's examination policy, its examination staff may be confused about their responsibilities.

In addition, the FDIC's policy and procedures also do not set management's expectations as to when IT examinations workpapers must be uploaded to RADD. Specifically, the FDIC's examination policy states that examiners "should scan documents within a reasonable time after receiving or developing them."

Without complete and timely IT examination workpapers in RADD, the FDIC's ability to manage, oversee, and audit its IT examination process is limited. Specifically, the FDIC's ICRS cannot ensure InTREx examinations are being performed in compliance with policies and procedures. Further, the lack of complete documentation hinders the ability to conduct reviews of IT examination operations and limits the transparency of IT examination operations. Finally, FDIC and State agency examiners may not be able to leverage workpapers or records from previous years' examinations when planning future IT examinations. Reviewing prior year workpapers provides FDIC examiners with an opportunity to understand past issues

and is also useful in examination planning.[63] Therefore, it is important for the FDIC to have clear policies and procedures for how and when workpapers should be filed.

Recommendations

We recommend that the Director, RMS:

11. Develop and implement examination policy and procedures to designate the roles and responsibilities for filing and maintaining IT examination workpapers in RADD.

12. Develop and implement procedures and controls to ensure that workpapers are properly filed in RADD in accordance with the FDIC's examination policy and procedures.

13. Establish and document the timeframe for uploading IT examination workpapers to RADD.

The FDIC Lacks Procedures to Ensure That IT Examiners Review Threat Information Affecting Banks

GAO Internal Control Standards state that organizations should document policies that define responsibilities for achieving operational process objectives and addressing related risks. According to the Internal Control Standards, individuals serving in key roles may further define policies through day-to-day procedures. In addition, policies and procedures serve as an important control for ensuring that processes are repeatable, consistent, and disciplined.

Further, our recent OIG report titled *Sharing of Threat Information to Guide the Supervision of Financial Institutions*[64] stated that for threat information to be actionable, it must be disseminated to the right people, in the right format, and at the right time. Policies and procedures help to ensure the effective dissemination of threat information to those who need it. We found that the FDIC did not have effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions.

[63] According to our survey, 223 of 273 respondents (or 82 percent) stated that reviewing prior examination workpapers is an important resource when conducting IT examinations.
[64] FDIC OIG, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (AUD-22-003) (January 2022).

The FDIC shares threat information with examination personnel through the RMS collaborative platform. Specifically, the Critical Infrastructure Resilience Team (CIRT) within the RMS Operational Risk group acquires and analyzes information about threats that can affect insured financial institutions.[65] The threat information comes from external sources, such as government agencies, including the DHS, the Federal Bureau of Investigation, and the Department of the Treasury. In addition, the FDIC uploads its Operational Risk Book to the RMS collaborative platform, which is a quarterly publication that provides a high-level summary of IT-related supervisory risks in banks. The book covers operational, IT, and electronic payment risks and trends identified in banks and service providers.

The collaborative platform also maintains Risk Advisories (RA) and Technical Examination Aids (TEA), which are developed by examiners and used to communicate emerging risks and assist examiners in evaluating these risks. RAs are developed by examination staff and approved by the RMS IT Supervision Branch before distribution. In addition to the RA, examiners can also develop TEAs, which provide guidance on how to assess the risk areas discussed in an RA. The RA process is intended to be dynamic and provide examination staff opportunities to provide input when they identify new or emerging risks.

Examination staff use the resources available on the RMS collaborative platform to ensure that examiners can assess whether financial institutions identify and effectively address IT and cybersecurity. However, we found that the FDIC has not established procedures for examiners in reviewing and utilizing the threat information on the platform.

We interviewed four examiners who were each unaware of any guidance or expectation as to whether examination staff were required or expected to review the threat information on the collaborative platform. As a result, we found that examiners are inconsistent in the frequency in which they reviewed threat information:

- Two examiners stated that they reviewed the threat information on the RMS collaborative platform at least quarterly;
- Two examiners did not regularly review threat information; and
- One examiner was unaware that threat information was maintained on RMS's collaborative platform.

[65] The RMS CIRT is responsible for advising RMS management on cybersecurity and critical infrastructure-related issues to facilitate RMS and financial services sector preparedness and resilience. The team researches, assesses, and disseminates to supervisory personnel operational threat information affecting the banking sector, financial institutions, and their service providers.

According to officials within the RMS Operational Risk group, examiners are expected to review the threat information on the collaborative platform, but the FDIC has not established guidance or required examiners to do so on a defined basis. In addition, the RMS CIRT sends examiners weekly emails that highlight alerts, advisories, and publications from DHS and other sources. However, these emails from the FDIC's CIRT are only sent to a limited group of RMS examiners, ITEAs, and ITCAs. Specifically, only 34 percent (362 of 1,060) of RMS personnel that can lead or participate on IT examinations receive the weekly emails.[66] According to RMS officials, weekly CIRT emails are directed to examiners who are assigned more frequently to IT examinations.

RMS IT Supervision Branch officials stated that they conducted a presentation at a conference in May 2022 to encourage examination staff to review and utilize the threat information available on the collaborative platform. However, we found that the conference was intended for RMS staff who primarily conduct or support IT examinations. As a result, only 27 percent (283 of 1,060) of RMS personnel that can lead or participate on IT examinations attended the conference.

By not establishing guidance through policies and procedures, examiners are not aware of management's expectations or requirements to review threat information, and thus are not held accountable to do so. According to GAO's Internal Control Standards, policies and procedures also communicate management's directives to employees and help to ensure that employees properly carry out those directives. With the increasing number and types of IT and cyber threats to banks, it is imperative that examiners are properly prepared to identify and assess emerging threats and risks to banks and the financial sector.

Recommendations

We recommend that the Director, RMS:

14. Establish and implement procedures that define responsibilities for reviewing and applying threat information during IT examinations.

15. Provide training for applying threat information during IT examinations.

[66] The total of 1,060 personnel includes the number of RMS's commissioned risk management examiners (as of March 31, 2022), ITEAs (as of March 31, 2022), and ITCAs (as of June 23, 2022).

The FDIC Should Expand Its Data Analytics to Improve the InTREx Program and Identify Emerging IT Risks

The FDIC is not fully utilizing available data and tools to improve the effectiveness of the InTREx program and identify emerging risks at financial institutions.

GAO Internal Control Standards direct management to establish activities to monitor performance measures and indicators. Monitoring performance helps ensure that an organization achieves its objectives. Management can use performance measures and indicators to perform analysis and take appropriate action when needed. In addition, in RMS's 2018-2022 Strategic Plan, the FDIC identified the need to leverage technology to improve the efficiency and effectiveness of its programs, provide effective examiner tools, and enhance analytical capability to assess industry and institution risks.

The FDIC issues quarterly reports on the InTREx program. These reports are available to all management and examination staff, and include metrics to monitor performance, such as changes in URSIT ratings across supervisory regions and the average number of examination and pre-planning hours. However, these reports are limited to data within the ViSION system[67] and do not analyze other available InTREx data. For example, the ViSION system does not capture the details within examination procedures and decision factor summaries.

In 2017, the FDIC developed a tool to conduct analysis of unstructured data from examinations called AlphaRex. In 2018, RMS used AlphaRex to analyze InTREx examination workpapers and ROEs across multiple IT examinations to identify opportunities for improvement to the InTREx program. Specifically, the tool was used to analyze areas of program performance such as the rates of responses to examination procedures, the impact of decision factors on the component rating, and trends in examiner decision factor ratings. These results were shared with the InTREx Interagency Committee and used in part to update the examination procedures and decision factors in the S&D Core Module. Since that time, the FDIC has continued to ingest IT examination data but has not used AlphaRex to develop additional analysis of InTREx data.

[67] FDIC OIG, *Reliability of Data in the FDIC Virtual Supervisory Information on the Net System* (EVAL-22-001) (November 2021) found data reliability concerns with the examination completion date and mail date fields within ViSION.

According to FDIC officials within the RMS IT Supervision Branch, AlphaRex has also been used to identify financial institutions at risk from zero-day attacks.[68] For example, the FDIC deployed AlphaRex when the "Spectre" and "Meltdown"[69] vulnerabilities were announced to identify financial institutions with patch management risks. Based upon the use of this tool, the FDIC was able to identify and contact susceptible financial institutions to help ensure their systems and networks were patched in response to these new threats. Expanding the use of AlphaRex to analyze IT examination data unique to the FDIC can similarly improve the InTREx program and identify emerging trends, threats, and IT risks. For example, the AlphaRex tool could be used to identify potential IT risk trends by ingesting and analyzing additional data sources.

We identified a similar finding in our OIG Report, *Sharing of Threat Information to Guide the Supervision of Financial Institutions*.[70] Specifically, we found that RMS was not performing trend analysis of data collected by FDIC examiners such as those available in electronic documents and other supervisory records in RADD, nor had they established procedures to guide its analysis. Such analysis could be valuable to both policy makers and examiners in assessing cyber threats, formulating supervisory strategies, and evaluating the adequacy of InTREx procedures and examiner training.

In addition, in 2015, the GAO found that financial regulatory agencies (including the FDIC) were only collecting and analyzing limited information from IT examinations. Specifically, based on deficiencies identified in individual examinations, the GAO found that the financial agencies (including the FDIC) were not aggregating and analyzing data from across the banking sector.[71] Further, the financial agencies did not have standardized methods for collecting examination data that could allow them to readily analyze trends across institutions. The GAO concluded that without collecting and analyzing data consistently, regulators did not obtain information that could identify broader IT issues affecting their regulated entities, and better target their IT risk assessments. As a result, the GAO recommended that the FDIC and other Federal regulatory agencies should routinely categorize IT examination

---

[68] NIST defines a zero-day attack as an attack that exploits a previously unknown hardware, firmware, or software vulnerability. See NIST Internal Report 8011 Vol. 3, *Automation Support for Security Control Assessments Software Asset Management* (December 2018).
[69] On January 3, 2018, the National Cybersecurity and Communications Integration Center became aware of a set of security vulnerabilities—known as Spectre and Meltdown—that affected modern computer processors. These vulnerabilities could be exploited to steal sensitive data present in a computer system's memory.
[70] FDIC OIG, *Sharing of Threat information to Guide the Supervision of Financial Institutions* (AUD-22-003) (January 2022).
[71] GAO, *CYBERSECURITY Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information* (July 2015).

findings and analyze this information to identify trends that can guide areas of review across institutions. In May 2017, the GAO subsequently closed the recommendation to the FDIC.

By further utilizing the AlphaRex tool, the FDIC could improve the InTREx program and become better positioned to effectively identify trends and promote risk remediation efforts. These analyses could further increase the FDIC's ability to identify patterns in problems across institutions, which could result in better targeted reviews and the assignment of IT experts among their staff.

Recommendations

We recommend that the Director, RMS:

16. Conduct a review to determine areas in which the AlphaRex tool could be utilized to identify areas of improvement for the InTREx program and emerging IT risks and trends at financial institutions.

The FDIC Needs to Establish Performance Goals, Objectives, and Measures for Its InTREx Program

The GAO stated that performance goals and objectives, and related performance measures, serve as important management tools for planning Federal programs and initiatives.[72] According to the GAO, program goals and objectives communicate the results that agencies seek from their programs. Performance measures demonstrate the progress agencies make toward achieving program goals and objectives. Performance measures provide agency managers with crucial information to identify gaps in program performance, and to plan any needed improvements. The GAO's Internal Control Standards recognize performance goals and objectives and related measures as key components of an effective internal control system.

Each year, the FDIC develops FDIC Performance Goals (FPG) to focus the Agency's attention on fulfilling its core mission responsibilities and highest priority initiatives. In 2021, the FDIC identified several FPGs that focused on improving its supervision program. However, these goals did not focus on IT supervision activities and did not

[72] For example, see GAO reports, entitled *Federal Buildings, GSA Should Establish Goals and Performance Measures to Manage the Smart Buildings Program* (Report No. GAO-18-200) (January 2018); *Performance Measurement and Evaluation: Definitions and Relationships* (Report No. GAO-11-646SP) (May 2011); and *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making* (Report No. GAO-05-927) (September 2005).

address the performance of IT examinations or the effectiveness of the InTREx Program.

In addition to FPGs, FDIC Divisions and Offices also establish goals and objectives at the Division or Office level, such as performance goals that focus on the effectiveness of RMS's supervision program. Specifically, in its Strategic Plan 2018-2022, RMS established the following performance goal: "RMS supervision is effective, forward-looking, and provides value-added risk management expertise to banks." However, this goal does not directly address the FDIC's InTREx program.

In addition, RMS has provided no way to measure this goal, and it has not provided a way to gauge the FDIC's progress towards reaching this outcome.

In relation to the goal, RMS established strategic objectives (see Table 2).

Table 2: RMS Strategic Plan 2018-2022 Goal One and Strategic Objectives

Goal: RMS supervision is effective, forward-looking, and provides value-added risk management expertise to banks.	
Strategic Objective 1.1	RMS's supervision program reflects the lessons learned from past crises.
Strategic Objective 1.2	RMS's supervisory activities are risk-focused and driven by bank business model and risk profile.
Strategic Objective 1.3	RMS provides clear, consistent, meaningful, and timely guidance to the industry.

Source: 2018-2022 RMS Strategic Plan.

However, these strategic objectives do not identify measures or indicators needed to assess whether the goal or the underlying strategic objectives have been achieved. Importantly, neither the goal nor the underlying objectives address the FDIC's IT examination program. According to RMS officials, RMS has not established separate action items or metrics under its strategic plan since 2018.

Without establishing IT examination performance goals, objectives, and metrics, the FDIC is unable to measure the effectiveness of the InTREx program. Further, the FDIC is unable to determine whether its IT examination activities under the InTREx program are achieving their desired outcomes or results. Establishing and implementing performance goals and objectives, and associated measures, instill accountability in Federal programs and initiatives, and promote transparency regarding management's expectations for results.

Recommendations

We recommend that the Director, RMS:

17. Develop and implement defined, objective, quantifiable, and measurable goals related to the InTREx program.

18. Develop and implement a process to collect and analyze relevant data regarding the InTREx program.

19. Develop and implement metrics and indicators, including outcome measures, to assess the effectiveness of the InTREx program and to determine if the program is achieving its desired results and outcomes.

FDIC COMMENTS AND OIG EVALUATION

On January 20, 2023, the FDIC Director, Division of Risk Management Supervision, provided a written response to a draft of this report, which is presented in its entirety in Appendix 5. In its response, the FDIC acknowledged the OIG's recommended improvements to the InTREx program and stated it has begun certain improvements to address the OIG's recommendations.

The FDIC noted that it reviewed each of the criticized IT examinations in the OIG's sample and concurred with the IT ratings in all but one case. In this one case, the FDIC acknowledged that "the examination materials could support one lower component and composite rating." Nevertheless, the FDIC stated it "confirmed that the FDIC's information technology (IT) examinations are high quality [and] produce accurate ratings…." The FDIC also stated it "…found no evidence of ineffective InTREx implementation of the InTREx Program," despite the multiple instances of non-compliance with InTREx procedures and examination policy, as well as the lack of guidance, review processes, and training identified by the OIG.

The FDIC's response dismissed the report's findings and attempted to minimize the significance of the report's recommendations. Out of 10 sampled IT examinations, identifying even one examination with an inaccurate URSIT rating is significant, and clearly supports the OIG's conclusion that the FDIC needs to improve its InTREx program to effectively assess and address IT and cyber risks at financial institutions. Notwithstanding the FDIC's concurrence with the majority of OIG recommendations, the FDIC's response failed to fully acknowledge the shortcomings identified in our report and focus on improving the InTREx program. Although the FDIC concluded that the change in ratings for the one examination would not affect the bank's insurance premiums, similar deficiencies in another examination could. Further, the limited sample size and high number of deficiencies identified within the IT examinations sampled collectively demonstrate the need for the FDIC to establish additional or enhance current IT examination controls to improve the effectiveness of the InTREx program.

The FDIC concurred with 16 of 19 report recommendations and partially concurred with 3 recommendations. The FDIC's proposed corrective actions were sufficient to address 14 of the 19 recommendations, and the FDIC plans to complete corrective actions for these recommendations by December 31, 2023. We consider these 14 recommendations to be resolved.

However, we found the corrective actions outlined by the FDIC did not fully satisfy the remaining five recommendations (Recommendations 5, 7, 17, 18 and 19) and as a result, these recommendations are considered unresolved:

- **Recommendation 5.** The FDIC concurred with Recommendation 5. The FDIC's proposed actions include reminding staff of the importance of the InTREx workpaper procedures and reviewing current controls for improvements. However, the FDIC's current controls consist primarily of reviewing a small sample of examinations after these examinations have been completed. Implementing controls that ensure examiners complete examination procedures and decision factors prior to the completion of IT

examinations would provide increased assurance that examinations are completed properly, and reduce the need to rescind ratings or adjust a bank's insurance premiums.

- **Recommendation 7.** The FDIC concurred with Recommendation 7. The FDIC acknowledged that in its review of the IT examinations sampled, one IT examination supported a lower component and composite rating. The FDIC concluded that no corrective action is necessary solely because the change would not have an effect on the bank's insurance premiums; however, no detailed information was provided to support the FDIC's review or this decision. A change in ratings may require actions such as an update to the bank's examination records in ViSION and RADD, and notifications to the financial institution and other stakeholders.

- **Recommendations 17, 18, and 19.** The FDIC partially concurred with Recommendations 17, 18, and 19. However, the FDIC's proposed actions do not fully address these recommendations, which include establishing performance goals and metrics specific to the FDIC's InTREx program, and collecting relevant data to measure the effectiveness of the program in achieving its desired results and outcomes. The FDIC stated that "RMS will continue to set defined, quantifiable, and measureable goals related to IT examinations, including the cybersecurity component of IT examinations, in the FPGs and Annual Performance Plan." However, as noted in our report, these goals are broad and do not measure the performance of IT examinations nor are they specific to the InTREx program. By developing goals at the programmatic-level, the FDIC can help to instill accountability in the InTREx program and promote transparency regarding management's expectations for results.

For these five unresolved recommendations, we will work with the FDIC during the audit follow-up process to seek resolution. All of the recommendations in this report will remain open until we confirm that corrective actions have been completed and the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 6.

Objective

The objective of this audit was to determine whether the FDIC's Information Technology Risk Examination (InTREx) program effectively assesses and addresses IT and cyber risks at financial institutions.

We conducted this performance audit from April 2021 through November 2022 in accordance with generally accepted government auditing standards (2018 version).[73] These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Scope and Methodology

The scope of our audit focused on the design and implementation of the FDIC's InTREx program. Specifically, we assessed the FDIC's InTREx procedures against Federal guidance, other regulatory agency IT examination procedures, and industry best practices. In addition, we evaluated whether IT examinations were performed consistent with the FDIC's examination policies, InTREx procedures, and other guidance. Further, we assessed the FDIC's processes for improving its InTREx program and examination activities.

The audit did not assess whether examiners had accurately identified all IT and cyber risks but whether IT examinations had been performed in accordance with FDIC policies and procedures. In addition, the audit did not assess the effectiveness of the FDIC's IT training programs to prepare examiners for leading and performing IT examinations at financial institutions.

To obtain an understanding of the FDIC's InTREx program and address the audit objective, we interviewed FDIC personnel from the Division of Risk Management Supervision (RMS), including the RMS Director, the Deputy Director of RMS's Operational Risk group, and officials from the IT Supervision Branch and Operations Branch. We also interviewed RMS examination field staff and officials from the Chief Information Officer Organization. In addition, we reviewed relevant FDIC policies, procedures, and guidance, including:

- FDIC RMS Regional Director (RD) Memoranda:

[73] In April 2021, the Comptroller General of the United States issued technical updates to the 2018 generally accepted government auditing standards which became effective upon issuance. Because we initiated this audit in November 2020, we followed the 2018 standards. The technical updates did not impact the results of our audit.

    - Information Technology Risk Examination (InTREx) Program, 2016-009-RMS (June 2016);
    - Information Technology and Operations Risk On-the-Job Training Programs, 2019-025-RMS (September 2019);
    - Scanning Policy for Electronic Workpaper Documentation, 2013-008-RMS (September 2013);
- RMS Risk Management Manual of Examination Policies (updated October 2022);
- RMS Case Manager Procedures Manual (updated February 2021);
- InTREx Interagency Committee Charter (October 2016); and
- FDIC Formal and Informal Enforcement Actions Manual (November 2019).

To develop criteria for assessing the effectiveness of the InTREx program, we used the FDIC RD Memoranda, Risk Management Manual of Examination Policies, and InTREx Interagency Committee Charter. We supplemented the FDIC's internal documents with the following Federal Regulations, Federal Standards, and industry best practices:

- 12 CFR Appendix B to Part 364 – Interagency Guidelines Establishing Information Security Standards (January 2022);
- GAO Standards for Internal Control in the Federal Government (Internal Control Standards) (September 2014);
- Federal Financial Institutions Examination Council Information Technology Examination Handbook;
- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (April 2018); and
- Center for Internet Security Critical Security Controls v.8 (May 2021).

We used the GAO Internal Control Standards as the primary criteria for assessing the effectiveness of the FDIC's InTREx program. The Internal Control Standards define 17 specific principles that are necessary to establish an effective internal control system at Federal agencies. Our audit assessed certain attributes pertaining to 12 of these 17 principles. The report findings present the internal control deficiencies we identified pertaining these twelve principles. Because we limited the scope of our work to 12 of the 17 principles, the audit may not have identified all internal control deficiencies existing at the time of our work.

Additionally, we considered the following recent OIG and GAO reports:

- OIG Report, *The FDIC's Implementation of Supply Chain Risk Management* (EVAL-22-003) (March 2022);
- *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (February 2021 and February 2022);

- OIG Report, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (AUD-22-003) (January 2022);
- GAO Report, *Cybersecurity – Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Useable Threat Information* (GAO-15-509) (July 2015); and
- GAO Report, *Bank Supervision – FDIC Could Better Address Regulatory Capture Risks* (GAO-20-519) (September 2020).

To further assess the effectiveness of the InTREx program, we judgmentally selected and evaluated a sample of 10 IT examinations conducted during the period of January 1, 2020 to December 31, 2020 against RMS's examination policy and InTREx procedures. The sample included at least one examination at each of the six supervisory regions and covered examinations at the three InTREx Complexity Levels: A, B, and C. Additionally, we reviewed the training records for examiners with an Intermediate or Advanced IT SME designation to ensure compliance with their respective ongoing IT training requirements.

We conducted a survey of FDIC personnel who led or participated in IT examinations to obtain their perspectives on the design and implementation of the InTREx program, and gain insights on examiner training, program challenges, and areas for improvement. To obtain a survey population, the OIG used the FDIC's ViSION application to identify examiners who were assigned the IT EIC role for IT examinations during the period of January 1, 2020 to June 30, 2021. In addition, on August 19, 2021, we obtained a list of ITEAs and ITCAs. On August 23, 2021, we sent the voluntary survey to the 804 FDIC personnel. On September 3, 2021, the OIG closed the survey with responses received from 317 of 804 FDIC examiners and IT examination support staff, reflecting a 39-percent response rate.[74]

We also interviewed financial regulatory agency officials from the Federal Reserve Board, Office of the Comptroller of the Currency, and National Credit Union Administration to understand their process for conducting IT examinations, including their implementation of the InTREx program, if applicable. In addition, we obtained information from the Conference of State Bank Supervisors on how state banking regulatory agencies implemented the InTREx program.

We did not rely on computer processed information to accomplish our audit objective. We determined that information system controls were not significant to the audit objective and, therefore, we did not evaluate the overall effectiveness of information system controls. We corroborated information to support our audit

[74] We did not perform steps to assess the statistical reliability of the survey results. Throughout this report, we summarize the actual responses received, and do not project the survey results to the total population of FDIC IT examiners and analysts.

conclusions with information from various sources, including supporting documentation, and testimonial evidence from subject matter experts. In addition, we assessed the risk of fraud and abuse related to our objective in the course of evaluating audit evidence.

Appendix 2 Acronyms and Abbreviations

CFR	Code of Federal Regulations
CIOO	Chief Information Officer Organization
CIRT	Critical Infrastructure Resilience Team
CSBS	Conference of State Bank Supervisors
DHS	Department of Homeland Security
DIF	Deposit Insurance Fund
EIC	Examiner-in-Charge
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FPG	FDIC Performance Goal
FRB	Federal Reserve Board
FSOC	Financial Stability Oversight Council
GAO	Government Accountability Office
GPRAMA	Government Performance and Results Act Modernization Act of 2010
ICRS	Internal Control and Review Section
Interagency Guidelines	Interagency Guidelines Establishing Information Security Standards
InTREx	Information Technology Risk Examination Program
IT	Information Technology
ITCA	IT Cyber Analyst
ITEA	IT Examination Analyst
ITEC	IT Examination Course
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OJT	On-the-Job Training
RA	Risk Advisory
RADD	Regional Automated Document Distribution and Imaging system
RD	Regional Director
RMS	Division of Risk Management Supervision
ROE	Report of Examination
SME	Subject Matter Expert
TEA	Technical Examination Aid
TSP	Technology Service Provider
URSIT	Uniform Rating System for Information Technology
ViSION	Virtual Supervisory Information on the Net

Appendix 3 Summary of Sample Testing Results

The table below summarizes the deficiencies identified from our sample testing described in our report. Specifically, we assessed a sample of 10 IT examinations against RMS's IT examination-related policy and procedures. For each sample item, we indicated with a "checkmark" instances in which we identified the following: 1) incomplete examination procedures in the InTREx Core Modules, 2) decision factors not assessed in the InTREx Core Modules, 3) outdated workpapers, and 4) whether all workpapers were filed in RADD (RMS's examination workpaper system-of-record). See Appendix 1, *Objective, Scope, and Methodology* for additional details on our sampling methodology.

	Incomplete Examination Procedures	Decision Factors Not Assessed	Outdated Examination Workpapers	Workpapers Not Filed in RADD
Sample 1	✓			
Sample 2	✓	✓	✓	✓
Sample 3			✓	
Sample 4	✓	✓		✓
Sample 5	✓	✓		
Sample 6	✓			✓
Sample 7	✓			
Sample 8				
Sample 9	✓	✓		✓
Sample 10				✓

Appendix 4 Examiner and Non-Examiner Titles and Descriptions

This table provides titles and descriptions of the FDIC's commissioned examiners and specialized IT examination support staff who may lead or support InTREx examinations.

Title	Description
Risk Management Examiner	Commissioned examiner who has completed baseline IT training and a 90-day IT examination rotation. Risk management examiners can only lead InTREx Level C examinations (lowest complexity level).
Intermediate IT SME	Risk management examiner who graduated from the Intermediate IT OJT program. Intermediate IT SMEs can lead InTREx Level B and C examinations.
Advanced IT SME	Risk management examiner who graduated from the Advanced IT OJT program. Advanced IT SMEs can lead InTREx Level A, B, and C examinations.
IT Examiner	Senior examiner with advanced IT skills and experience. IT Examiners typically lead InTREx Level A examinations.
IT Examination Analyst	Senior non-examiner with specialized IT skills. ITEAs perform a variety of administrative, technical, analytical, and advisory duties. ITEAs can support InTREx Level A, B, and C examinations.
IT Cyber Analyst	Non-examiner with entry-level IT skills. ITCAs are required to complete an extensive training program, established by RMS, to further develop their IT and cyber-related skills. ITCAs can support InTREx Level A, B, and C examinations.

Federal Deposit Insurance Corporation

MEMO

TO: Terry L. Gibson
Assistant Inspector General, Audits, Evaluations, and Cyber
Office of Inspector General

FROM: Doreen R. Eberley
Director, Division of Risk Management Supervision

DOREEN EBERLEY Digitally signed by DOREEN EBERLEY Date: 2023.01.20 12:49:18 -05'00'

CC: E. Marshall Gentry, Chief Risk Officer
Lisa K. Roy, Acting Deputy Director and Chief of Staff, Division of Risk Management Supervision
Martin D. Henning, Deputy Director, Division of Risk Management Supervision
William H. Henley Jr, Associate Director, Division of Risk Management Supervision

DATE: January 20, 2023

RE: Draft Audit Report Entitled *Implementation of the FDIC's InTREx Program* (Assignment No. 2021-004)

The FDIC has completed its review of the Office of Inspector General's (OIG) draft audit report titled "Implementation of the FDIC's InTREx Program" (No. 2021-004) issued on December 16, 2022. FDIC management concurs with 16 of the report's 19 recommendations, and partially concurs with three recommendations. We provide a full response to the audit findings and recommendations below.

Our work to support this audit confirmed that the FDIC's information technology (IT) examinations are high quality, produce accurate ratings, identify weaknesses in IT risk management, and that the FDIC holds banks accountable for addressing those weaknesses. Although the draft audit report's Executive Summary concludes in part – "Without effective implementation of the InTREx program, significant IT and cyber risks may not be identified by examiners and addressed by financial institutions" – we found no evidence of ineffective InTREx implementation that led to the outcomes listed, nor is such evidence provided in the draft audit report. In fact, two independent FDIC employees reviewed each of the criticized IT examinations in the OIG's sample and concurred with the IT ratings in all but one case. In that one case, independent reviewers concluded the examination materials could support one lower component and composite rating. However, even if those ratings were lower, they would not have affected the bank's insurance premiums as the draft audit report stated was possible.

Nevertheless, the audit recommended improvements in InTREx administration such as updating references in InTREx materials, communicating InTREx changes to examiners better, and filing workpapers more consistently. The FDIC has begun certain improvements and provides estimated completion dates for OIG's recommendations below.

FDIC Federal Deposit Insurance Corporation

Management Response to the OIG Findings and Recommendations

1. **Finding** – The InTREx program is outdated and does not reflect current Federal guidance and frameworks for three of four InTREx Core Modules.

   Recommendation 1: We recommend that the Director, RMS update and implement the InTREx program to reflect current IT and cyber risks and guidance.

   Recommendation 2: We recommend that the Director, RMS work with the InTREx Interagency Committee to develop and implement procedures to govern the process to update the InTREx program.

   Management Decision: Concur

   Planned Action: InTREx is current consistent with its purpose and design. RMS designed InTREx to change infrequently, and to be high-level so that it is useful in examining all banks. It focuses on controls that do not change as frequently as threats or technology generally. For example, InTREx does not contain hyperlinks that are prone to breaking. However, readers' searches on InTREx key words take them straight to underlying, current, and more detailed materials.

   The InTREx Interagency Committee considers InTREx updates when underlying materials change, particularly when new, effective controls are identified. This practice is consistent with the InTREx Interagency Committee charter.

   Relative to recommendation one, RMS will review the InTREx RD Memorandum (RD Memorandum 2016-009-RMS) to identify any updates needed consistent with InTREx design and purpose, will publish those updates, and will communicate these changes to examiners prior to the changes taking effect.

   Relative to recommendation two, RMS will review the InTREx Interagency Committee charter to identify any changes needed, consistent with InTREx design and purpose. For example, RMS will review the charter's effectiveness in specifying what change types the Committee should be monitoring for their impact on InTREx. Since the InTREx Interagency Committee charter can only be changed after three, independent groups (FDIC, Board of Governors of the Federal Reserve System, and state banking departments) reach agreement, implementing any changes needed to the charter are likely to require additional time beyond the estimated completion date below.

   Estimated Completion Date: September 30, 2023

2. **Finding** – The FDIC did not communicate or provide guidance to its examiners after updates were made to the program.

   Recommendation 3: We recommend that the Director, RMS communicate updates to the InTREx program to examiners in a timely manner and prior to implementation.

   Recommendation 4: We recommend that the Director, RMS issue revised or updated guidance to examiners to address InTREx program updates.

   Management Decision: Concur

   Planned Action: RMS is preparing InTREx changes unrelated to this audit. RMS will combine these

Federal Deposit Insurance Corporation

unrelated changes with any changes resulting from the review identified above. RMS will issue revised or updated guidance, as necessary, and communicate all of these changes to examiners prior to the changes taking effect.

Estimated Completion Date: September 30, 2023

3. **Finding** – FDIC examiners did not complete InTREx examination procedures and decision factors required to support examination findings and URSIT ratings.

   Recommendation 5: We recommend that the Director, RMS develop and implement control mechanisms to ensure that examiners complete examination procedures and decision factors.

   Recommendation 6: We recommend that the Director, RMS review the sampled examinations in which examination procedures and decision factors were not completed in order to determine whether or not the ratings are accurate.

   Recommendation 7: We recommend that the Director, RMS take corrective actions to address any inaccuracies identified as a result of the review recommended above.

   Management Decision: Concur

   Planned Action: Regarding recommendations six and seven, RMS reviewed the OIG-sampled examinations where the draft report states procedures and decision factors were not completed. In eight of the nine examinations, two independent FDIC reviewers (individuals uninvolved in the original examination completion and review) confirmed the accuracy of the URSIT ratings. In the one remaining examination, independent reviewers concluded the examination materials could support one lower component and composite rating. However, even if those ratings were lower, they would not have affected the bank's insurance premiums as the draft audit report stated was possible. No corrective action is necessary.

   The OIG draft report criticizes procedure comments not existing in seven examinations sampled. In the examinations criticized, decision factor comments provided relevant information about the procedures completed.

   The OIG draft report criticizes the fact that in four examinations the examiner or analyst did not check workpaper decision factor checkboxes. In each of these four cases, the examiner or analyst provided written comments so that the reader can identify the decision factor quality level concluded (which should have also been indicated by checking the box).

   Regarding recommendation five, RMS will remind examiners and analysts of the importance of the InTREx workpaper procedures.

   All regions have controls to ensure that examiners or analysts complete necessary examination procedures and decision factors. RMS provided written evidence of these controls to the OIG in November 2022. RMS will review these controls to identify any needed improvements relative to the finding.

   RMS headquarters staff also conduct periodic regional reviews to, in part, assess the adequacy of regional procedures. RMS will include reviews of InTREx procedure and decision factor completion in

Federal Deposit Insurance Corporation

regional review scopes. RMS will share future InTREx workpaper exceptions from regional reviews with all regions.

Estimated Completion Date: June 30, 2023

4. **Finding** – The FDIC has not employed a supervisory process to review IT workpapers prior to the completion of the examination, in order to ensure that findings are sufficiently supported and accurate.

   Recommendation 8: We recommend that the Director, RMS update and implement examination policy and InTREx procedures to require that IT examination workpapers be reviewed for adequacy and that workpapers sufficiently support examination conclusions prior to the issuance of the ROE.

   Recommendation 9: We recommend that the Director, RMS share the results of ICRS Regional Reviews with all supervisory regions.

   Management Decision: Concur

   Planned Action: The Risk Management Manual of Examination Policies (Manual) instructs examiners and analysts in completing an examination. In Section 1.1 – Basic Examination Concepts and Guidelines the Manual states in part "The examiner-in-charge is responsible for ensuring that only appropriate electronic workpapers are retained and that the workpapers are retained in accordance with existing policies and procedures."

   The RMS Director conveys more detailed instructions to examiners and analysts through RD Memoranda. RD Memorandum 2013-008-RMS titled "Scanning Policy for Electronic Workpaper Documentation" states in part

   > "Examiners must exercise sound judgment in determining which electronic workpapers to retain at the conclusion of an examination or other supervisory activity. Retained documents should support examination and verification procedures performed, conclusions reached, and assertions of fact or opinion detailed in Reports of Examination or other supervisory findings. Examiners should retain only final documents (not multiple versions of a document) and delete all other documents that are not needed to support the findings. The examiner-in-charge is responsible for ensuring that only appropriate electronic workpapers are retained for examinations or other supervisory activities in accordance with existing policies and procedures."

   Regarding recommendation eight, RMS is updating examiner instructions that address workpaper review roles and responsibilities, and will implement any needed changes relative to the finding.

   Regarding recommendation nine, RMS will share future InTREx workpaper exceptions from regional reviews with all regions.

   Estimated Completion Date: December 31, 2023

5. **Finding** – The FDIC does not offer training to reinforce InTREx program procedures to promote consistent completion of IT examination procedures and decision factors.

Federal Deposit Insurance Corporation

Recommendation 10: We recommend that the Director, RMS provide refresher training to reinforce InTREx program procedures, such as the completion of all examination procedures and decision factors, and address updates and changes to the InTREx program.

Management Decision: Concur

Planned Action: In 2019 RMS provided examiners an update on InTREx as part of the Commissioned Examiner Training class. Staff provided course materials to the OIG on July 21, 2022. RMS held virtual All-Staff Training Days on October 13, 2021 (course materials were provided to OIG August 19, 2022), and June 29, 2022 (course materials were provided to OIG July 21, 2022) that included reinforcement of IT examination procedures. RMS regional offices provide InTREx refresher training for examiners in each region.

RMS will review each regional office's refresher training materials and change them when necessary to be consistent with InTREx instructions regarding completion of procedures and decision factors.

RMS will continue to include IT examination components in all-staff training, as appropriate.

Estimated Completion Date: June 30, 2023

6. **Finding** – FDIC's examination policy and InTREx procedures were unclear which led examiners to file IT examinations workpapers in an inconsistent and untimely manner.

Recommendation 11: We recommend that the Director, RMS develop and implement examination policy and procedures to designate the roles and responsibilities for filing and maintaining IT examination workpapers in RADD.

Recommendation 12: We recommend that the Director, RMS develop and implement procedures and controls to ensure that workpapers are properly filed in RADD in accordance with FDIC's examination policy and procedures.

Recommendation 13: We recommend that the Director, RMS establish and document the timeframe for uploading IT examination workpapers to RADD.

Management Decision: Concur

Planned Action: RMS has policies and procedures that designate the roles and responsibilities for filing and maintaining all examination workpapers in RADD, controls for ensuring examiners properly file workpapers, and an instruction to examiners on when to upload workpapers to RADD.

The Risk Management Manual of Examination Policies (Manual) instructs examiners and analysts in completing an examination. In Section 1.1 – Basic Examination Concepts and Guidelines the Manual states in part "The examiner-in-charge is responsible for ensuring that only appropriate electronic workpapers are retained and that the workpapers are retained in accordance with existing policies and procedures."

The RMS Director conveys more detailed instructions to examiners and analysts through RD Memoranda. RD Memorandum 2013-008-RMS titled "Scanning Policy for Electronic Workpaper

FDIC Federal Deposit Insurance Corporation

Documentation" states in part

> "Examiners must exercise sound judgment in determining which electronic workpapers to retain at the conclusion of an examination or other supervisory activity. Retained documents should support examination and verification procedures performed, conclusions reached, and assertions of fact or opinion detailed in Reports of Examination or other supervisory findings. Examiners should retain only final documents (not multiple versions of a document) and delete all other documents that are not needed to support the findings. The examiner-in-charge is responsible for ensuring that only appropriate electronic workpapers are retained for examinations or other supervisory activities in accordance with existing policies and procedures."

RD Memorandum 2013-008-RMS also states in part "Examiners should scan documents in a secure location within a reasonable time after receiving or developing them."

RD Memorandum 2016-009-RMS titled "Information Technology Risk Examination (InTREx) Program" Appendix A – Examination Procedures states in part "Generally, support for examination findings should follow existing guidance in … Regional Director Memorandum 'Scanning Policy for Electronic Workpaper Documentation' dated September 23, 2013 (transmittal 2013-008). Documentation should be sufficient to support overall examination findings and recommendations and to provide a clear trail of decisions and supporting logic."

The regional workpaper controls referenced in response to Finding 3 include procedures to review workpaper filing, as do the periodic regional reviews.

Regarding recommendations 11 and 12, RMS will evaluate these policies, procedures, and controls for effectiveness and update them if necessary.

Regarding recommendation 13, RMS will specify further the timeframe for uploading IT examination workpapers to RADD in examiner instructions.

Estimated Completion Date: December 31, 2023

7. **Finding** – The FDIC does not provide guidance to examination staff on reviewing threat information to remain apprised of emerging IT threats and those specific to financial institutions.

   Recommendation 14: We recommend that the Director, RMS establish and implement procedures that define responsibilities for reviewing and applying threat information during IT examinations.

   Recommendation 15: We recommend that the Director, RMS provide training for applying threat information during IT examinations.

   Management Decision: Concur

   Planned Action: Examiners use multiple information types to understand examination context. The RMS staffing model takes into account time needed for information review.

Federal Deposit Insurance Corporation

Relative to recommendation 14, RMS will review the InTREx RD Memorandum (RD Memorandum 2016-009-RMS) and attachments, identify any needed change to guide examiner and analyst use of threat information in support of IT examinations, and implement those changes.

Relative to recommendation 15, RMS will review the curricula for the two IT examination courses all examiners attend (the "Information Technology Examination Course" and the "Introduction to Security Course") to determine whether they adequately highlight threat information availability and how to use threat information during IT examinations, and make any necessary changes.

RMS will continue to publish threat information to examiners who spend more of their time examining IT, and will continue to publish to all RMS employees information about the most significant threats.

RMS periodically provides training to all staff on how IT examination procedures relate to cybersecurity threats, and provides threat briefings to IT examiners and leaders more frequently. RMS will continue these practices, and will continue to highlight in these events the availability of additional threat information.

Estimated Completion Date: September 30, 2023

8. **Finding** – The FDIC is not fully utilizing available data and analytic tools to improve the InTREx program and identify emerging IT risks.

   Recommendation 16: We recommend that the Director, RMS conduct a review to determine areas in which the AlphaRex tool could be utilized to identify areas of improvement for the InTREx program and emerging IT risks and trends at financial institutions.

   Management Decision: Concur

   Planned Action: RMS uses various methods to evaluate InTREx effectiveness in differentiating among examined institutions' IT risk management practices for purposes of improving InTREx. RMS uses various methods to also understand emerging IT risks and trends at financial institutions. For example, in 2021 and 2022 RMS horizontally reviewed ransomware attacks at FDIC-supervised institutions. The FDIC wanted to understand the threat better, and learn about the defensive techniques that were most helpful in defending against those attacks. RMS will continue to use what it views as the most effective methods for understanding emerging IT risks and trends at financial institutions.

   RMS will review its use of AlphaRex and identify any needed change relative to the finding.

   Estimated Completion Date: December 31, 2023

9. **Finding** – The FDIC has not established goals and performance metrics to measure its progress in implementing the InTREx program.

   Recommendation 17: We recommend that the Director, RMS develop and implement defined, objective, quantifiable, and measurable goals related to the InTREx program.

   Recommendation 18: We recommend that the Director, RMS develop and implement a process to collect and analyze relevant data regarding the InTREx program.

FDIC Federal Deposit Insurance Corporation

Recommendation 19: We recommend that the Director, RMS develop and implement metrics and indicators, including outcome measures, to assess the effectiveness of the InTREx program and to determine if the program is achieving its desired results and outcomes.

Management Decision: Partially concur

Planned Action: RMS identifies goals and performance metrics relative to supervising risk management rather than relative to the workprograms and other tools it uses to supervise risk management. Following are examples of goals and performance metrics relevant to IT risk management.

The 2021 FDIC Performance Goals (FPGs) contained the following goals focused on IT supervision activities: 1.02.e Develop a position paper on concentration risks associated with cloud providers; 1.03.c Implement a computer security incident notification final rule; and 1.03.d Complete a horizontal review of significant service providers using the Focused Advanced Cyber Threat (FACT) work program.

The 2022 FPGs additionally contain the following goals focused on IT supervision activities: 1.01.d Complete a horizontal review of significant service providers to assess operational resilience; 1.01.e Implement procedures for sharing threat and vulnerability information with FDIC staff, and amplifying others' messages to banks, and service providers; 1.01.f Complete FDIC-supervised ransomware attack horizontal review; and 1.01.g Review and revise as necessary interagency protocols for addressing severe cybersecurity incidents.

The FDIC also creates an Annual Performance Plan that contains goals focused on IT supervision activities.

- The 2021 Annual Performance Plan 2.1-4 states: Implement strategies to promote enhanced cybersecurity and business continuity within the banking industry. This Goal has related metrics to measure success: enhance the cybersecurity awareness and preparedness of the banking industry; continue to conduct horizontal reviews that focus on the IT risks in large, complex institutions and service providers; continue to use the Cybersecurity Examination Program for service provider examinations, including the most significant service provider examinations; and implement a computer security incident notification final rule.
- The 2022 Annual Performance Plan Goal 2.1-4 states: Implement strategies to promote enhanced cybersecurity and business continuity within the banking industry. This Goal has related metrics to measure success: continue to conduct horizontal reviews that focus on the IT risks in large, complex institutions and service providers; and continue to conduct service provider examinations using the Cybersecurity Examination Program.

Relative to recommendations 17, 18, and 19, RMS will continue to set defined, quantifiable, and measurable goals related to IT examinations, including the cybersecurity component of IT examinations, in the FPGs and Annual Performance Plan. The existing processes to collect and analyze relevant data will be used. Similarly, the existing metrics and indicators that include measurable outcomes will be used.

Estimated Completion Date: March 31, 2023

8

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 will review the InTREx RD Memorandum to identify any updates needed, consistent with InTREx design and purpose. RMS will publish those updates, and will communicate these changes to examination staff prior to these changes taking effect.	September 30, 2023	$0	Yes	Open
2	The FDIC will review the InTREx Interagency Committee Charter to identify changes needed, consistent with InTREx design and purpose.	September 30, 2023	$0	Yes	Open
3	The FDIC will issue revised or updated guidance, as necessary, and communicate these changes to examination staff prior to the changes taking effect.	September 30, 2023	$0	Yes	Open
4	See response to Recommendation 3.	September 30, 2023	$0	Yes	Open
5	The FDIC's proposed corrective action does not fully satisfy the recommendation.		$0	No	Open
6	The FDIC reviewed the OIG-sampled examinations where the draft report states procedures and decision factors were not completed to determine whether ratings were accurate.	June 30, 2023	$0	Yes	Open
7	The FDIC's proposed corrective action does not fully satisfy the recommendation.		$0	No	Open
8	The FDIC will update examiner instructions that address workpaper review roles and responsibilities, and will implement any needed changes relative to the finding.	December 31, 2023	$0	Yes	Open
9	The FDIC will share future InTREx workpaper exceptions from regional reviews with all regions.	December 31, 2023	$0	Yes	Open
10	The FDIC will continue to provide IT examination training as part of its all-staff training, as appropriate. In addition, RMS will review each regional office's refresher training materials to be consistent with InTREx instructions regarding the completion of procedures and decision factors.	June 30, 2023	$0	Yes	Open
11	The FDIC will evaluate its IT examination workpaper filing policies,	December 31, 2023	$0	Yes	Open

	procedures, and controls for effectiveness, and update them, if necessary.				
12	See response to Recommendation 11.	December 31, 2023	$0	Yes	Open
13	The FDIC will specify further the timeframe for uploading IT examination workpapers to RADD in examiner instructions.	December 31, 2023	$0	Yes	Open
14	The FDIC will review the InTREx RD Memorandum and attachments to identify and implement changes to guide examination staff on the use of threat information in support of IT examinations, as appropriate.	September 30, 2023	$0	Yes	Open
15	The FDIC will review the curriculum for required IT examination courses to determine whether training adequately highlights threat information availability and guidance on using threat information during IT examinations.	September 30, 2023	$0	Yes	Open
16	The FDIC will review its use of AlphaRex and identify any needed changes relative to the finding.	December 31, 2023	$0	Yes	Open
17	The FDIC's proposed corrective action does not fully satisfy the recommendation.		$0	No	Open
18	The FDIC's proposed corrective action does not fully satisfy the recommendation.		$0	No	Open
19	The FDIC's proposed corrective action does not fully satisfy the recommendation.		$0	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.