Security Controls Over the Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System

June 2020 **AUD-20-004**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

Executive Summary

Security Controls Over the Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its mission. As of February 11, 2020, the FDIC maintained 274 information systems, nearly half of which contained sensitive information and Personally Identifiable Information (PII). One of these systems is the Regional Automated Document Distribution and Imaging System (RADD). RADD serves as the official recordkeeping and electronic filing system for the FDIC's supervisory business records.

RADD contains over 5 million electronic supervisory business records. These records include confidential bank examination reports that contain supervisory ratings; examination work papers that include detailed financial information about bank customers; and other sensitive information submitted by systemically important financial companies. RADD documents often contain sensitive PII, including names, addresses, citizenship status, Social Security Numbers, and bank account numbers for bank employees and customers. The large amount of sensitive information in RADD underscores the need for effective security controls that mitigate the risk of security incidents, such as breaches.

The FDIC Office of Inspector General engaged the professional services firm of Cotton & Company LLP to conduct the audit. The audit objective was to assess the effectiveness of selected security controls for protecting the confidentiality, integrity, and availability of information in RADD. The audit assessed security controls in eight areas covered in National Institute of Standards and Technology (NIST) guidance: Plans of Action and Milestones (POA&Ms), Configuration Management, Access Management, Removable Media, Encryption, Audit Logging, Security Authorization and Continuous Monitoring, and Contingency Planning.

Results

The FDIC's controls and practices were effective in five of the eight security control areas assessed. Specifically, the FDIC addressed RADD security weaknesses consistent with POA&M guidance; assessed and approved configuration changes to RADD; restricted the use of removable media; authorized RADD to operate and

monitored critical security controls; and developed and tested a contingency plan for RADD.

However, controls and practices in the remaining three security control areas were not fully effective either because they did not comply with FDIC policy requirements or because they were not implemented in a manner consistent with relevant NIST security guidance. Specifically, the FDIC did not:

- Use a secure encryption solution to protect RADD data as recommended by NIST;
- Implement a control to prevent unauthorized access to sensitive documents in RADD that had not yet been indexed with metadata. Metadata is information used by RADD to control user access to documents; or
- Adequately document roles, responsibilities, and procedures for reviewing and maintaining RADD audit logs as recommended by NIST.

Weaknesses related to Encryption and Access Management increased the risk of unauthorized access to sensitive information, including PII. The lack of documented roles, responsibilities, and procedures for Audit Logging caused the FDIC to be dependent upon the knowledge and experience of a limited number of staff.

Recommendations

The report contains two recommendations to: (1) implement a control to prevent RADD users from accessing sensitive documents that have not been indexed with metadata; and (2) define and update roles, responsibilities, and procedures for reviewing and maintaining RADD audit logs. The report does not contain recommendations pertaining to encryption, because Cotton & Company LLP confirmed that the FDIC took corrective action during the audit to address the encryption weakness identified.

In a written response to a draft of the report, the FDIC concurred with both recommendations and described corrective actions it took to address the recommendations. Prior to finalizing our report, we confirmed that the FDIC's corrective actions were responsive and closed both recommendations.

Contents

Part I

☆☆☆☆☆☆☆☆

Report by Cotton & Company LLP

SECURITY CONTROLS OVER THE FEDERAL DEPOSIT INSURANCE CORPORATION'S REGIONAL AUTOMATED DOCUMENT DISTRIBUTION AND IMAGING SYSTEM AUDIT REPORT

JUNE 23, 2020

Cotton & Company LLP
635 Slaters Lane
Alexandria, Virginia 22314
703.836.6701 | 703.836.0941, fax
lschwartz@cottoncpa.com | www.cottoncpa.com

Table of Contents

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

Mark F. Mulholland
Assistant Inspector General for IT Audits and Cyber
Office of Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of Security Controls Over the Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System

Cotton & Company LLP is pleased to submit the attached report detailing the results of our performance audit of selected security controls over the Federal Deposit Insurance Corporation's (FDIC) Regional Automated Document Distribution and Imaging System. The FDIC Office of Inspector General engaged Cotton & Company LLP to conduct this performance audit pursuant to Contract Number CORHQ-15-G-0161. We performed the work from November 15, 2018 through September 24, 2019.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS 2011 Revision), as promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,
Cotton & Company LLP

Loren Schwartz, CPA, CISSP, CISA
Partner

Introduction

The Federal Deposit Insurance Corporation (FDIC) relies heavily on information systems to carry out its responsibilities of insuring deposits, supervising insured financial institutions, and resolving failed insured financial institutions. As of February 11, 2020, the FDIC maintained 274 information systems.[1] One of these systems is the Regional Automated Document Distribution and Imaging System (RADD). The FDIC developed RADD in 2008. RADD serves as the official recordkeeping and electronic filing system for supervisory business records used by the FDIC's Division of Risk Management Supervision (RMS) and Division of Depositor and Consumer Protection (DCP).[2]

According to RMS officials, RADD contains over 5 million electronic supervisory business records. These records include confidential bank examination reports that contain supervisory ratings; examination work papers that include detailed financial information about bank customers; sensitive information submitted by systemically important financial companies; and proposed supervisory and enforcement actions, such as civil money penalties against individuals. These documents often contain sensitive personally identifiable information (PII),[3] including names, addresses, citizenship status, Social Security Numbers (SSNs), and bank account numbers for bank employees and customers.

The large amount of sensitive information stored in RADD underscores the need for effective security controls that mitigate the risk of security incidents, such as breaches.[4] Breaches can expose individuals to identity theft or other types of consumer fraud, which can result in embarrassment, inconvenience, reputational harm, and financial loss. Breaches can also result in unnecessary costs, potential legal liability, and reputational harm for the FDIC. Further, the FDIC has identified RADD as a critical resource to achieving the FDIC's mission-essential functions.[5] Accordingly, a disruption to RADD's operation could impair the FDIC's ability to accomplish its mission of ensuring the safety and soundness of insured financial institutions.

Background

Approximately 3,500 employees and contractor personnel have some level of access to RADD.[6] The majority of these users are RMS and DCP examination staff in the FDIC's Washington, D.C., Regional, and Area Offices. Other RADD users include employees and contractors within the FDIC's Division of Resolutions and Receiverships, Division of Insurance and Research, Division of Complex Institution Supervision and Resolution, and Legal Division.

---

[1] According to the Enterprise Architecture Repository—the FDIC's authoritative source of information for its information systems.

[2] RMS conducts examinations of FDIC-supervised financial institutions to assess their overall financial condition, management practices and policies, and compliance with applicable laws and regulations. DCP conducts examinations of FDIC-supervised institutions to assess compliance with consumer protection laws and regulations and the extent to which the institutions meet community needs under the Community Reinvestment Act of 1977, 12 U.S.C. § 2901 *et seq*.

[3] Office of Management and Budget (OMB) Circular Number A-130, *Managing Information as a Strategic Resource* (OMB Circular A-130) (July 2016), defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." FDIC Circular 1360.9, *Protecting Sensitive Information* (April 2007), defines sensitive PII as a subset of PII that presents the highest risk of being misused for identity theft or fraud.

[4] According to OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 2017), a breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses [PII] or (2) an authorized user accesses or potentially accesses [PII] for an other than authorized purpose."

[5] FDIC 2017-2018 Business Process Analysis (BPA) / Business Impact Analysis (BIA) (July 2018).

[6] RADD User Listing (January 17, 2019).

RMS has primary responsibility for maintaining RADD. This includes implementing periodic changes to RADD's functionality, monitoring system logs for unusual or suspicious activity, providing users with training, and maintaining system documentation. The Division of Information Technology (DIT)—a component within the Chief Information Officer (CIO) Organization—has responsibility for maintaining the underlying information technology (IT) infrastructure on which RADD operates. The IT infrastructure includes, for example, the servers[7] that process and store RADD data, the laptops and desktops that individuals use to access RADD, and the network security controls that RADD relies on for safe and reliable operation. The CIO Organization also maintains a backup data center in Dallas, Texas, that provides restoration capabilities in the event RADD becomes unavailable.

RADD Access Management

RMS also has responsibility for managing user access for RADD. According to RMS policy,[8] only employees and contractor personnel with a legitimate business need for supervisory business records may access RADD. In addition, RADD users may access only those documents within the system that are commensurate with the users' job functions and business needs. To address these policy requirements, system administrators in RMS, known as RADD Administrators, assign users to one of four groups within the Microsoft Windows Active Directory (Active Directory).[9] Each of these Active Directory groups provides a baseline level of functionality and security access permissions for RADD users. **Table 1** summarizes the functionality, permissions, and total number of individuals associated with each Active Directory Group.

[7] According to NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, a server is a computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).
[8] RMS/DCP Regional Directors Memorandum, *Regional Automated Document Distribution and Imaging System* (July 2019).
[9] Active Directory is a product of the Microsoft Corporation that consists of several services that run on the Windows Server operating system to manage permissions and access to networked resources. Individuals must have an FDIC network account to be included in the Active Directory.

Table 1: RADD Active Directory Groups

Active Directory Group	Functionality and Permissions	Total Individuals*
1. User	This group provides users the ability to read, download, and print RADD documents.	3,331
2. Index	This group provides users the ability to import documents into RADD and tag each document with metadata (i.e., identifying information, such as the document's name, location, type, source, and date). The process of tagging documents with metadata is known as Indexing.	104
3. Administrator	This group provides users with elevated permissions to create and remove accounts, manage user access, monitor and investigate suspicious activity, and perform system maintenance and troubleshooting.	40
4. Design	This group provides users with the highest level of permissions. In addition to Administrator permissions, users in the Design Group have control over all aspects of RADD functionality, including the ability to implement system changes.	2

*Figures are as of January 17, 2019.
Source: Cotton & Company's review of RADD security documentation and discussions with RMS and DIT personnel.

After assigning users to an Active Directory Group, RADD Administrators further restrict the functionality and access permissions of users by assigning them to a specific role in RADD based on their job title (e.g., RMS Examiner, DCP Examiner, IT Examiner, Case Manager, etc.). RADD Administrators also assign users to a geographic profile in RADD that restricts the users' access to documents within the users' geographic location. For example, users in the FDIC's New York Regional Office can generally only access documents of financial institutions under the purview of the New York Regional Office. RADD Administrators can implement additional access restrictions based on specific business needs or a user's particular circumstances.

In addition, RADD Administrators can prohibit a user from accessing specific documents if the user has reported a conflict of interest. A conflict of interest may arise, for example, if an FDIC-supervised institution employs an examiner's spouse or family member. In this case, the examiner would have a conflict of interest with respect to reviewing documents related to the institution.

Users can locate documents in RADD through a file directory on the system's homepage or by using the system's search function. When a user attempts to access a document, RADD performs a series of security checks to determine whether the user has permissions to access the document. If a user does not have permissions to access a document in RADD, but has a legitimate business need to do so, the user may invoke a feature in RADD called "Auto Approve" if allowed by their access permissions.[10] Auto Approve prompts the user to enter a business reason for accessing the document and provides the user immediate access to the document for a period of 60 days. RADD sends an email to the user's

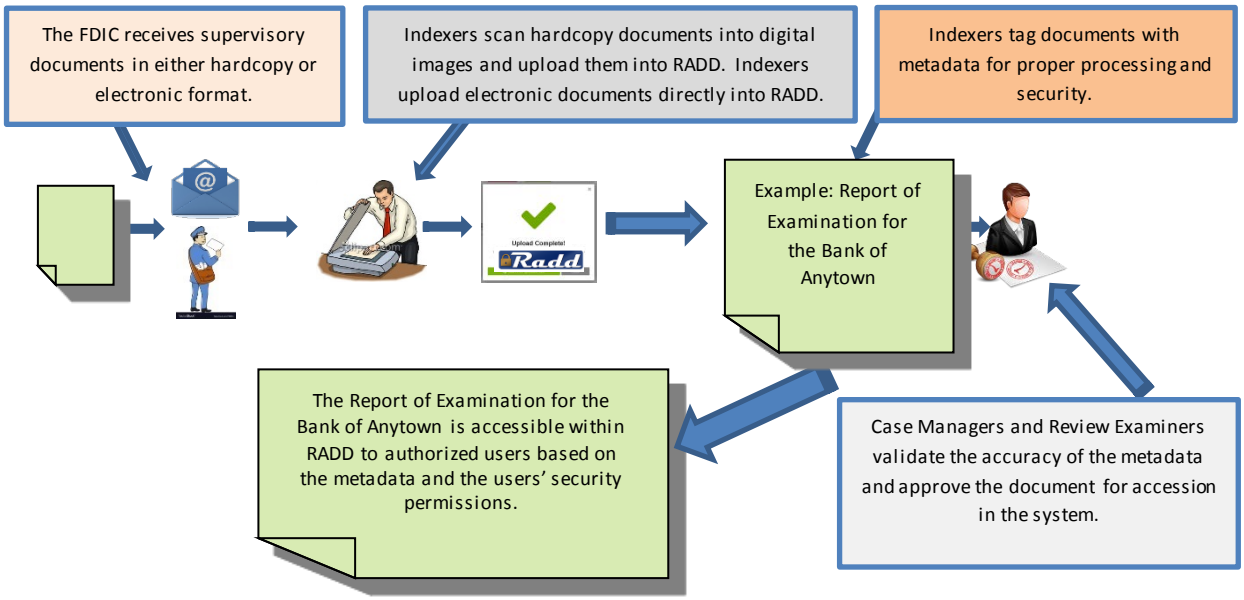
[10] RMS has developed a RADD Role-Based Security Matrix to document the access privileges associated with each role in RADD. According to the RADD Role-Based Security Matrix, 19 of the 34 roles in RADD allow for the use of the Auto Approve function.

supervisor and RADD Administrators, notifying them that the user has used Auto Approve to access the document. RADD maintains a log of these email notifications.

Scanning and Indexing Documents

Users in the Index Active Directory Group (Indexers) scan hardcopy documents into RADD using scanners in each of the FDIC's eight Regional and Area Offices. Indexers also upload electronic documents directly into RADD. Then, Indexers tag (or index) the documents with metadata (e.g., name, location, document type, source, and date). RMS Case Managers and DCP Reviewers validate the accuracy of the metadata assigned to each document. The accurate application of metadata to documents is critical, as RADD uses the metadata to organize and store documents in the system and to control user access to the documents. **Figure 1** illustrates the scanning and indexing process.

Figure 1: The RADD Scanning and Indexing Process



Source: Cotton & Company's review of the RADD User Manual (Version 6.28.18) and RMS policy.

Federal Security Requirements and Guidelines

The Federal Information Security Modernization Act of 2014 (FISMA)[11] requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems. FISMA directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information and information systems. NIST establishes required security standards in Federal Information Processing Standards (FIPS) Publications.[12] NIST supplements these standards with recommended guidelines in Special Publications (SPs).[13] NIST Special Publication (SP)

[11] Pub. L. No. 113-283 (December 2014). The FDIC has determined that FISMA is legally binding on the FDIC.
[12] The FDIC has determined that FIPS Publications are not binding on the Corporation because the Secretary of Commerce, who approves FIPS Publications, does not have the authority to impose mandatory requirements on the FDIC. Nevertheless, the FDIC views FIPS Publications as guidance for "best practices" in implementing security measures for information systems.
[13] The FDIC has determined that NIST SPs contain statements of best practices or guidance and are not binding on the FDIC.

800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013, updated January 2015), provides Federal agencies with a framework for protecting the confidentiality, integrity, and availability[14] of their information and information systems.

Certain Controls Assessed

From November 2018 to September 2019, we assessed the effectiveness of certain security controls for RADD in eight areas covered by NIST SP 800-53, Rev. 4. We identified these eight security control areas because we determined that a failure in the design or implementation of controls in these areas could impair the FDIC's ability to ensure the confidentiality, integrity, and availability of information in RADD. It could also jeopardize the FDIC's ability to achieve its strategic objective of examining and supervising financial institutions for safety and soundness, and consumer protection. **Table 2** describes the security control areas we assessed.

Table 2: Security Control Areas Assessed

Control Area	Definition
1. **Plans of Action and Milestones (POA&Ms)**	A POA&M is a management tool used to track the progress of corrective actions pertaining to security weaknesses found in programs and information systems. POA&Ms identify tasks that need to be accomplished, resources required to accomplish those tasks, and estimated completion dates.
2. **Configuration Management**	Configuration management refers to establishing and maintaining the integrity of IT products and information systems. Organizations foster integrity by controlling the processes for initializing, changing, and monitoring the configurations of those products and systems.
3. **Access Management**	Access management involves ensuring that only authorized users have access to IT resources and that access is limited to the minimum necessary for job performance.
4. **Removable Media**	Removable media consists of portable storage devices, such as Universal Serial Bus (USB) drives and Digital Versatile Disks (DVDs). Users can use removable media to copy or remove data from computing devices.
5. **Encryption**	Encryption is a process that scrambles information to make it unintelligible. Decryption converts encrypted data back into its original form so it can be understood.
6. **Audit Logging**	An audit log is a record of events occurring within an information system or network. Events can include, for example, password changes, failed logins, or use of administrative privileges. Reviewing audit logs can identify security incidents, such as policy violations, and operational problems that need to be addressed.
7. **Security Authorization and Continuous Monitoring**	Security authorization refers to accepting the risk of operating an information system based on a review of the system's security posture. Continuous monitoring refers to maintaining an ongoing awareness of information security, vulnerabilities, and threats to support risk management decisions.
8. **Contingency Planning**	A key component of contingency planning is developing and testing system contingency plans designed to recover and restore systems in the event of a disruption. Contingency plans help to ensure the availability of critical IT resources and continuity of operations in an emergency.

Source: Cotton & Company's review of guidance issued by OMB and NIST.

[14] According to FISMA, confidentiality means, "preserving authorized restrictions on [information] access and disclosure, including means for protecting personal privacy and proprietary information;" integrity means, "guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;" and availability means, "ensuring timely and reliable access to and use of information."

Audit Objective

We conducted this performance audit to assess the effectiveness of selected security controls for protecting the confidentiality, integrity, and availability of information in RADD.

Performance Audit Results

We determined that the FDIC's controls and practices were effective in five of the eight security control areas assessed. However, controls and practices in the remaining three security control areas were partially effective because the controls and practices did not comply with FDIC policy requirements or their implementation was not consistent with relevant NIST security guidelines. **Table 3** identifies the security control areas we assessed and our determinations regarding their effectiveness. A description of our results for each security control area follows the table.

Table 3: Effectiveness of Security Controls and Practices by Control Area

Security Control Area	Audit Result
Encryption	Partially Effective
Access Management	Partially Effective
Audit Logging	Partially Effective
POA&Ms	Effective
Configuration Management	Effective
Removable Media	Effective
Security Authorization and Continuous Monitoring	Effective
Contingency Planning	Effective

Source: Cotton & Company's review and analysis of selected security controls for RADD.
Note: Determinations of Effective indicate substantial compliance and/or consistency with relevant Federal and FDIC security requirements and guidelines. Determinations of Partially Effective indicate compliance and/or consistency with some, but not all, security requirements and guidelines. Determinations of Not Effective indicate substantial non-compliance and/or inconsistency with security requirements and guidelines.

Encryption

Encryption is a process intended to safeguard sensitive information from unauthorized disclosure or modification. Encryption involves converting information and data into an unreadable form or code so that unauthorized users cannot access the underlying information or data. Decryption involves converting encrypted information back to its original form so it can be understood. DIT implemented an encryption protocol called Transport Layer Security (TLS) in order to encode the information in RADD during transmission over the FDIC's network.

NIST SP 800-52, Rev. 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* (April 2014), provides Federal agencies with guidance on how to configure and implement TLS. NIST SP 800-52, Rev. 1, states that organizations should use Version 1.1 of TLS (or a newer version) to encrypt sensitive information. According to NIST, using earlier versions (prior to Version 1.1) of TLS is risky, because they are susceptible to cyberattacks.

On March 28, 2019, we observed two users access RADD: a local user in the Washington, D.C. metropolitan area and an out-of-area user in the FDIC's Kansas City Regional Office. We noted that RADD data involving the Washington, D.C. user was encrypted with a NIST-recommended version of TLS (version 1.2). However, RADD data involving the Kansas City user was encrypted with TLS version 1.0. As noted above, NIST has indicated that the TLS version 1.0 is an outdated encryption protocol that Federal agencies should not use to encrypt sensitive information.

According to DIT staff, DIT had configured its network equipment supporting Washington, D.C. users to use a NIST-recommended version of TLS. However, DIT had configured its network equipment supporting users outside of the Washington, D.C. metropolitan area with an outdated version of TLS. The FDIC did not report any security incidents during our audit due to the use of an outdated version of TLS. However, the use of TLS version 1.0 presented a risk that an unauthorized user could exploit known security vulnerabilities associated with this encryption protocol to intercept and read sensitive RADD information.[15]

In April 2019, after we identified the use of an outdated version of TLS on the FDIC's network, DIT staff provided us with documentation to support that they had upgraded TLS to a NIST-recommended version. We reviewed this documentation and confirmed that DIT had implemented an updated version of TLS. Therefore, we are not making a recommendation pertaining to Encryption.

Access Management

NIST SP 800-53, Rev. 4, recommends that organizations implement the security principle of "least privilege." The principle refers to the security objective of restricting user access to only those IT resources needed to perform official duties. In addition, FDIC Circular 1360.9, *Protecting Sensitive Information* (April 2007), states that only those individuals who have a legitimate need to access sensitive information in the performance of their duties shall be provided access. Further, RMS policy states that "RADD users will have permission to access only the documents commensurate with their job functions and business needs."[16]

[15] NIST SP 800-52, Rev. 1, discusses the vulnerabilities that can allow unauthorized access to information encrypted with TLS version 1.0.
[16] RMS/DCP Regional Directors Memorandum, *Regional Automated Document Distribution and Imaging System* (July 2019).

As discussed in the Background section of this report, RMS implemented role-based access controls to restrict the functionality and access permissions of RADD users in order to enforce the security principle of least privilege. However, we found that users could circumvent these access controls for documents that had been scanned into the system, but not yet indexed (that is, tagged with metadata). Any user with access to RADD could view and download these documents without restriction and without providing a justification, including users with security permissions that would normally prevent them from reviewing the documents. For example, any user could view documents for financial institutions that would normally be restricted to executive management due to their sensitivity, or for which the users had reported a conflict of interest.[17] The RADD search function allowed users to locate these documents by entering a date range for scanned documents as the search criteria.

We reviewed documents that Indexers had scanned into RADD, but not yet indexed over a four-day period. The total number of documents in this status ranged from 355 documents to 514 documents. Working in coordination with the FDIC Office of Inspector General (OIG), we identified confidential reports of examination that included supervisory ratings[18] and customer names associated to adversely classified loans.[19] We also identified documents that included the names, SSNs, and personal financial statements for bank officials and trustees. In addition, we identified correspondence associated to an individual seeking a waiver under Section 19 of the Federal Deposit Insurance (FDI) Act that detailed the full name, address, prior income, prior work history, and criminal history of the applicant.[20]

RADD did not restrict user access to these documents, because Indexers had not applied the required metadata to the documents by completing the indexing process. Without complete metadata, RADD defaulted to allowing all users access to the documents. The lack of access control over these documents increased the risk of unauthorized access to sensitive information and an insider threat,[21] which could have led to a cyber security incident.

We recommend that the Director, RMS:

1. Implement a control to prevent RADD users from accessing sensitive documents that have not been indexed with metadata.

In response to our identification of this issue, on September 12, 2019, RMS officials advised that they had implemented a system modification on August 26, 2019, to restrict user access to documents in RADD that had not been indexed. Prior to finalizing our audit report, the FDIC OIG confirmed that the system modification effectively addressed the access vulnerability identified during the audit.

[17] We reviewed a listing of all reported computer security incidents associated to RMS, DCP, and the FDIC's former Office of Complex Financial Institutions, provided by DIT covering the period July 1, 2018 to March 27, 2019 and found no incidents involving unauthorized access to sensitive RADD documents.

[18] Federal and state regulatory agencies, including the FDIC, use a standard system known as the Uniform Financial Institutions Rating System to assign supervisory ratings to insured financial institutions.

[19] According to the FDIC's Risk Management Manual of Examination Policies, reports of examination are "highly confidential" and subject to the confidentiality rules imposed by Part 309, *Disclosure of Information*, of the FDIC's Rules and Regulations.

[20] Section 19 of the FDI Act, 12 U.S.C. §1829, prohibits individuals convicted of certain criminal offenses from participating in the affairs of an insured depository institution without the prior written consent of the FDIC.

[21] According to FDIC Directive 1600.7, *FDIC Insider Threat and Counterintelligence Program*, an insider threat is a threat posed to the FDIC or U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any United States Government resource. This threat can include damage through espionage, terrorism, sabotage, unauthorized disclosure of classified information or unclassified sensitive information, or through the loss or degradation of FDIC resources or capabilities.

Audit Logging

NIST SP 800-53, Rev. 4, recommends that organizations review and analyze information system audit records (logs) for indications of inappropriate or unusual activity. NIST SP 800-92, *Guide to Computer Security Log Management* (September 2006), provides organizations with guidance for developing, implementing, and maintaining effective log management practices.[22] NIST SP 800-92 recommends that organizations develop policies, procedures, and standard processes for performing log management, including roles and responsibilities for key personnel. According to NIST SP 800-92, routine log analysis can identify security incidents, policy violations, fraudulent activity, and operational problems that need to be addressed. These NIST guidelines also emphasize the importance of clearly defining requirements for securing, retaining, and disposing of audit logs because they may contain sensitive information with privacy or security implications.

RMS developed the RADD Audit Manual (October 2016) to define audit logging policies, procedures, and processes for RADD. Based on our review of the RADD Audit Manual, and discussions with RMS personnel, we learned that RADD Administrators used three principal types of logs to monitor activity within the system:

(1) **Imperva Logs.**[23] RADD Administrators review Imperva Logs on a weekly basis to monitor activities in RADD's databases, such as changes to the databases and attempts to access the databases.

(2) **Application Programming Interface (API)[24] Logs**. RADD Administrators review API Logs to monitor user activities, such as attempts to exceed RADD's daily download limit[25] and the use of the Auto Approve function. RADD administrators receive email alerts when API log data meet predefined criteria.

(3) **Security Access Change Logs.** RADD Administrators review Security Access Change Logs to monitor changes in user accounts, such as the creation of new accounts and changes in account permissions. RADD administrators receive email alerts when Security Access Change Log data meet predetermined criteria.

[22] NIST SP 800-92 defines the term "log" as a record of events occurring within an organization's information systems and networks. Events can include, for example, password changes, failed logins, or failed accesses related to information systems, administrative privilege usage, or third-party credential usage. Logs consist of entries that contain information related to a specific event that has occurred within a system or network. Organizations identify those audit events that are significant and relevant to the security of their information systems and the environments in which those systems operate.

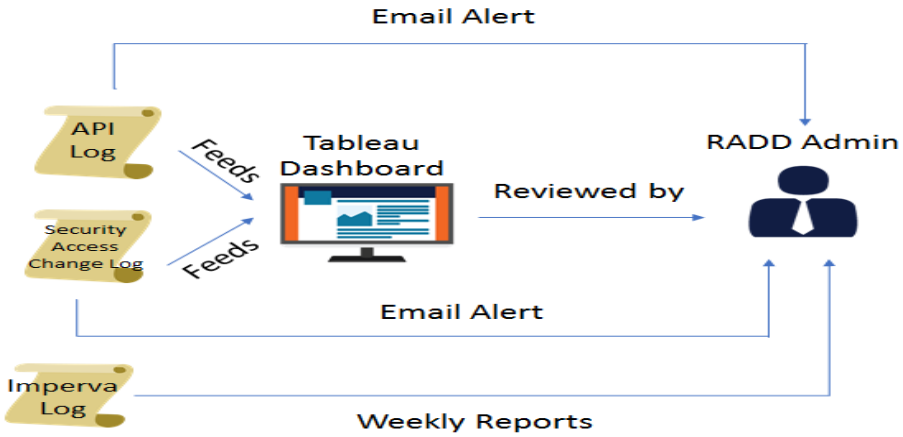
[23] According to the vendor's website, Imperva is a cyber security company that provides, among other products, system monitoring capabilities.

[24] NIST, in combination with other sources, defines the term API as a protocol intended to be used as an interface by software components to communicate with each other. In the case of RADD, the API receives user requests for document access and delivers the documents based on the privilege levels of each user.

[25] According to the RADD User Manual, RADD imposes a daily document download limit on users. Once a user reaches the download limit, RADD restricts the user's access to documents in the system for 24 hours.

RADD Administrators advised that they also use a Tableau[26] dashboard to monitor key metrics based on data from the API and Security Access Change logs. These key metrics include such things as: users who accessed and/or downloaded the largest number of documents in the last 7 days; users who made the most frequent use of the Auto Approve function within the last 7 days; the total number of denied access attempts; the top searches executed by users; and the most documents accessed for a financial institution. Collectively, the three types of logs described above and the Tableau dashboard are intended to help RADD Administrators monitor user access to ensure it is commensurate with business needs and that potentially suspicious activity is identified and investigated. **Figure 2** illustrates the audit logs and Tableau dashboard that RADD Administrators use to monitor RADD activities.

Figure 2: RADD Audit Logging Process



Source: Cotton & Company's review and analysis of the RADD's audit logging process.

We reviewed the RADD Audit Manual and found that it did not define key controls and procedures for audit logging, including:

- Use of the Tableau Dashboard by RADD Administrators to monitor key metrics;
- How RADD Administrators use information in the Imperva Logs to monitor database activity; and
- Roles and responsibilities for monitoring audit logs and following-up on suspicious activity.

In addition, the RADD Audit Manual did not define requirements for securing, retaining, and disposing of audit logs. According to NIST SP 800-92, defining such requirements reduces the risk of unauthorized access and manipulation, ensures compliance with legal or regulatory requirements (i.e., standard operational activities, incident handling, or investigations), and provides assurance that data will not be used beyond its intended business purpose. Additionally, according to NIST SP 800-92, a lack of detailed procedures for securing, retaining, and disposing of audit logs exposes organizations to increased risk of

[26] Tableau is a data visualization tool developed by a commercial vendor, Tableau Software.

inadvertent disclosures of sensitive information and compromises to the integrity of preserved evidence.

Up-to-date policies, procedures, and process documentation is an important internal control for ensuring that staff understand their roles and responsibilities and implement processes in a proper, consistent, and disciplined manner. The lack of documented policies, procedures, and processes for audit logging increased the operational risk associated with potential workforce staffing changes, because the FDIC was dependent on the knowledge and experience of a limited number of key staff.

We recommend that the Director, RMS:

2. Define and update roles, responsibilities, and procedures for reviewing and maintaining RADD audit logs.

As a result of our findings, RMS representatives advised us on September 12, 2019, that they updated the RADD Audit Manual on August 30, 2019, they updated the RADD Audit Manual to reflect the types of audit logs, reports, and alerts that RADD generates; and the frequency of the reviews performed. On May 21, 2020, RMS officials provided the FDIC OIG with a further updated version of the RADD Audit Manual, last revised September 24, 2019, to address the security, retention and disposal of audit logs. Prior to finalizing our audit report, the FDIC OIG confirmed that the updated RADD Audit Manual effectively addressed the audit logging concerns identified during the audit.

Plans of Action and Milestones

NIST SP 800-53, Rev. 4, recommends that organizations implement a process to ensure that organizations: develop and maintain POA&Ms for their information systems; document remedial actions to adequately respond to known risks; and report POA&M information. Without an effective process for managing POA&Ms, the FDIC may not devote adequate attention or resources to address known security weaknesses in RADD.

In April 2019, the CIO Organization issued a policy[27] that defines the FDIC's process for developing and maintaining POA&Ms and documenting remedial actions. The FDIC policy includes a requirement for staff to record and track POA&M information in an automated management tool. We reviewed POA&Ms addressing security weaknesses in RADD and confirmed that the POA&Ms contained recommendations, mitigation strategies, corrective actions, and milestones as prescribed by the CIO Organization's POA&M policy. We determined that the FDIC designed and implemented POA&Ms for RADD consistent with FDIC policy and NIST guidance.

Configuration Management

NIST SP 800-53, Rev. 4, recommends that agencies develop a configuration management plan that details the processes by which system changes are assessed, tested, and approved prior to implementation. NIST emphasizes the need to consider the potential impact any change has on

[27] CIO Organization Policy 19-001, *Policy on Management of Plan of Actions and Milestones*.

system security before it is implemented. Without effective configuration management, systems may not operate properly, stop operating altogether, or become vulnerable to security threats.

We confirmed that RMS personnel satisfied the requirement to develop a configuration management plan by formalizing the RADD Release Management Procedure to control configuration changes to the RADD application. The Release Management Procedure complemented DIT's Infrastructure Services Branch (ISB) Change Management Procedure.

Further, RADD Administrators used Team Foundation Server,[28] the FDIC's official change management tool, to maintain key information for all RADD changes between July 1, 2018 and February 6, 2019. This information included descriptions for each change, the code that was changed, and the time and names associated with key actions, such as change approvals and change deployments. We used information in the audit logs to conclude that all changes were tested and approved by appropriate personnel prior to implementation. We determined that the configuration management controls over RADD were designed, implemented, and operating in a manner consistent with NIST and FDIC guidance.

Removable Media

NIST SP 800-53, Rev. 4, recommends that organizations establish and implement a policy that addresses the protection of media, including removable media such as USB storage devices and DVDs. The use of removable media presents a risk of unauthorized exfiltration[29] of sensitive information. FDIC Directive 1300.4, *Acceptable Use Policy for FDIC Information Technology* (October 2018), prohibits users from downloading any data from any FDIC-furnished equipment to removable media unless an exception is granted. FDIC Directive 1300.4 defines the circumstances under which FDIC management may grant an exception. We confirmed that, as of March 28, 2019, all RADD users with the ability to use removable media had a written exception to do so. Therefore, we determined that the FDIC had designed and implemented removable media controls over RADD consistent with FDIC policy and NIST guidance.

Security Authorization and Continuous Monitoring

NIST SP 800-53, Rev. 4, recommends that organizations assign a senior-level executive or manager (Authorizing Official) to authorize an organization's information systems to operate.[30] NIST also recommends that organizations supplement system authorizations with continuous monitoring activities that include assessments of security controls to determine their effectiveness (i.e., whether the controls are implemented correctly). Absent an effective process for authorizing information systems, the FDIC cannot know whether the risk of operating RADD is acceptable, or whether additional security controls are needed to reduce risk. Further, without effective

[28] According to Microsoft, the product vendor, Team Foundation Server, now called Azure DevOps Server, is a set of collaborative software development tools. These tools include functionality such as code version control, change testing, and progress tracking.
[29] According to NIST 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, exfiltration is the unauthorized transfer of information from an information system.
[30] The Authorizing Official reviews security-related information describing the security posture of an information system, and using that information, determines whether the risk to mission/business operations is acceptable. If the Authorizing Official determines that the risk is acceptable, then the official explicitly accepts the risk. At the FDIC, the CIO functions as the Authorizing Official.

continuous monitoring, the FDIC cannot maintain ongoing awareness of RADD security vulnerabilities and threats, which could increase the risk of security incidents.

We determined that the CIO authorized RADD to operate, and that the authorization remained in effect during our audit. In addition, the FDIC maintained a system security plan for RADD in accordance with NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (December 2018). The system security plan provided an overview of RADD security requirements and described the controls in place or planned for meeting those requirements. Authorizing officials and security control assessors rely on information in system security plans to assess risks and plan and conduct security assessments. Further, in April 2018, the FDIC completed a security controls assessment for RADD consistent with its written methodology.[31] Therefore, we determined that the FDIC authorized RADD and monitored security controls consistent with NIST and FDIC guidance.

Contingency Planning

NIST SP 800-53, Rev. 4, recommends that organizations develop contingency plans for their information systems as part of an overall program for achieving continuity of operations for mission/business functions. According to NIST SP 800-53, Rev 4, contingency plans should contain procedures for recovering and restoring information systems within a timeframe commensurate with the criticality of the business functions supported by the system. Further, NIST SP 800-53, Rev. 4, states that organizations should test their system contingency plans to determine their effectiveness. Without an effective contingency plan for RADD, the FDIC cannot be sure it can maintain or restore its mission-essential supervisory functions within established timeframes following an emergency.

We confirmed that the FDIC assessed the criticality of RADD and determined the timeframe the system could be inoperable before incurring unacceptable impacts to mission/business processes (maximum tolerable downtime). The FDIC also developed a contingency plan for RADD that listed key contingency personnel, identified a backup processing site, defined backup and recovery procedures, and established a testing schedule. In addition, in November 2018, the FDIC conducted a successful failover[32] test of RADD to confirm that the application could operate at the FDIC's backup processing site. Therefore, we determined that the FDIC established and implemented contingency planning controls for RADD consistent with NIST guidance.

Conclusion

The FDIC implemented a number of information security controls and practices to protect the confidentiality, integrity, and availability of information in RADD. However, security controls and practices in the areas of Access Management, Encryption, and Audit Logging were not fully effective. Our report includes two recommendations that, together with the corrective actions already taken by the FDIC, will strengthen the effectiveness of security controls and practices over RADD.

[31] The FDIC Information Security Risk Management (ISRM) Continuous Control Assessment (CCA) Methodology.
[32] NIST SP 800-53, Rev. 4, defines failover as the capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Appendix 1: Objective, Scope, and Methodology

The objective of this performance audit was to assess the effectiveness of selected security controls for protecting the confidentiality, integrity, and availability of information in RADD. Cotton & Company LLP conducted this performance audit in accordance with the 2011 revision[33] of the Generally Accepted Government Auditing Standards. 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our objective, we reviewed the security control catalog in NIST SP 800-53, Rev. 4, to identify security controls that we deemed critical to maintaining the confidentiality, availability, and integrity of RADD. We selected these controls because a failure in their design or implementation would impair the FDIC's ability to ensure the confidentiality, integrity, and availability of RADD and its data. It would also jeopardize the FDIC's ability to achieve its strategic objective of examining and supervising financial institutions for safety and soundness, and consumer protection. We then grouped these security controls in eight areas and assessed their effectiveness. We determined effectiveness by assessing compliance with relevant Federal and FDIC security requirements and consistency with relevant Federal security guidelines. Controls were effective if they complied with and/or were consistent with relevant Federal and FDIC security requirements and guidelines; partially effective if they complied with and/or were consistent with some, but not all, security requirements and guidelines; and not effective if they were in substantial non-compliance and/or inconsistent with security requirements and guidelines.

We evaluated the design, implementation, and operating effectiveness of selected controls within each of the eight security control areas by:

- Examining user and system documentation, such as the RADD User Manual (Version 6.28.18) and RADD Audit Manual (Version 11.04.16);
- Reviewing relevant FDIC policies, procedures, and guidance;
- Interviewing and corresponding with RMS personnel responsible for supporting and maintaining RADD;
- Observing system connectivity and output (e.g., system settings, user listings, and system and software change listings);
- Judgmentally selecting specific RADD users, Auto Approve requests, and audit log reviews to perform detailed validation tests to ensure that controls described in policy were effectively executed; and

[33] Cotton & Company LLP began this performance audit on November 13, 2018. The 2018 revision of GAGAS is effective for performance audits beginning on or after July 1, 2019.

- Evaluating audit logging tools, reports, and practices.

We supplemented NIST SP 800-53, Rev. 4, with FISMA, other NIST SPs, and other relevant criteria for securing Federal information and information systems. We discussed our preliminary exceptions and conclusions with representatives of the FDIC OIG and FDIC management throughout the audit. We received management responses to our recommendations; however, we did not audit those responses. **Appendix 2** provides a detailed description of the conclusions we reached in each security control area. We assessed the risk of fraud and abuse related to the audit objective in the course of evaluating audit evidence. We performed our work at the FDIC's Virginia Square offices in Arlington, Virginia.

Appendix 2: Control Conclusions

Table 4: Control Conclusions

Security Control Area	Control Description in NIST 800-53, Rev 4	Control Test Result	Security Control Area Conclusion
Encryption	Implements encryption in accordance with applicable federal laws, Executive Orders, directives, FDIC policies, regulations, and standards.	Partially Effective – Data communications between servers supporting RADD were properly encrypted. In addition, RADD data at rest (stored on the servers) was properly encrypted. However, data communications between RADD and users outside the Washington, D.C. metropolitan area were encrypted with an outdated version of TLS.	Partially Effective
Access Management	Requires approvals for requests to create information system accounts.	Effective – RMS requires management approval for all users prior to granting RADD access.	Partially Effective
	Creates, enables, modifies, disables, and removes information system accounts in accordance with FDIC policy.	Effective – RMS disables access for users if they no longer have a business need to access the application or have been inactive for a defined period.	
	Authorizes access to the information system based on (1) a valid access authorization and (2) intended system usage.	Effective – RMS requires management approval for all users prior to granting RADD access.	
	Separates the duties of individuals as defined by FDIC; documents separation of duties for individuals; and defines information system access authorizations to support separation of duties.	Effective – RMS defines standard roles within RADD to ensure that all users have appropriate privileges.	
	Employs the principle of least privilege, allowing only authorized access necessary for users to accomplish assigned tasks.	Partially Effective – RMS authorizes user access using least privilege principles. However, RADD users can bypass access restrictions for unindexed documents.	
	Reviews accounts for compliance with account management requirements.	Effective – RMS performs periodic RADD account reviews.	
Audit Logging	Develops, documents, and disseminates an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment,	Partially Effective – RMS developed the RADD Audit Manual that described	Partially Effective

	coordination among organizational entities, and compliance. Develops procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	auditable events and procedures for following up on potential exceptions. However, the manual did not document all audit logging capabilities or establish clear accountability for key responsibilities.	
	Determines that the information system is capable of auditing defined auditable events; coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and determines that FDIC identified events are to be audited within the information system along with the frequency of auditing for each identified event.	Effective – RMS provided log output, evidence of log review, and evidence of follow-up for suspicious log activity.	
POA&Ms	Develops POA&Ms for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies.	Effective – RMS established POA&Ms for RADD in accordance with CIO Organization policy and NIST guidance.	Effective
	Updates existing POA&Ms based on findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Effective – RMS incorporated recent RADD control assessment results into POA&Ms.	
Configuration Management	Develops, documents, and disseminates a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Develops procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	Effective – RMS established a configuration management plan for RADD that included change management responsibilities and procedures.	Effective
	Determines the types of changes to the information system that are configuration-controlled. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.	Effective – RMS defined the types of changes and the approval processes required for each change. RMS reviewed each change, including consideration for the security impact, prior to approving its implementation.	
	Analyzes changes to the information system to determine potential security impacts prior to change implementation.	Effective – RMS assessed the impact of all changes prior to implementation.	

Removable Media	Establishes and implements policy addressing the use of removable media.	Effective – FDIC established and implemented policy that only allows the use of removable media with specific management authorization for each user.	Effective
Security Authorization and Continuous Monitoring	Assigns a senior-level executive or manager as the authorizing official for the information system; ensures that the authorizing official authorizes the information system for processing before commencing operations; and updates the security authorization in accordance with FDIC policy.	Effective – The FDIC CIO authorized RADD to operate.	Effective
	Develops a continuous monitoring strategy and implements a continuous monitoring program that includes: establishment of metrics to be monitored; establishment of frequency for monitoring and performing assessments of defined items; ongoing security control assessments in accordance with the organizational continuous monitoring strategy; ongoing security status monitoring of organization-defined metrics in accordance with the continuous monitoring strategy; correlation and analysis of security-related information generated by assessments and monitoring; response actions to address results of the analysis of security-related information; and reporting the security status of the organization and the information system to FDIC-identified personnel.	Effective – RMS followed a Security Controls Assessment continuous monitoring strategy, which details the frequency and control scope of periodic assessments. The strategy also includes assessment responsibilities of key personnel. In addition, the strategy includes reporting requirements for deficient controls.	
Contingency Planning	Develops a contingency plan for the information system that: identifies essential missions and business functions and associated contingency requirements; provides recovery objectives, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented. Contingency plans are reviewed and approved by FDIC identified personnel and distributed to required personnel.	Effective – RMS developed a contingency plan that includes recovery and restoration procedures for RADD in the event of a disruption. The procedures are designed to ensure a timely recovery of the system to reduce a disruption's impact on essential business functions to an acceptable level. The plan lists the names, contact information, and responsibilities of key contingency planning personnel. The plan is reviewed by RMS, DCP, and DIT personnel and updated at a minimum annually.	Effective

	Plans for the resumption of essential missions and business functions within FDIC-defined time period of contingency plan activation.	Effective – RMS developed a contingency plan that considers the maximum tolerable downtime of RADD in its recovery and restoration procedures.
	Tests the contingency plan for the information system to determine the effectiveness of the plan and the organizational readiness to execute the plan; reviews the contingency plan test results; and initiates corrective actions, if needed.	Effective – DIT and RMS tested the contingency plan and documented and reviewed the test results.
	Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of essential missions/business functions within FDIC-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable; ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.	Effective – The FDIC established an alternate processing site for RADD and tested its failover capabilities.

Source: Cotton & Company's review and analysis of RADD based on NIST SP 800-53, Rev. 4.

Appendix 3: Acronym List

Table 5: Acronym List

Acronym	Description
API	Application Program Interface
BIA	Business Impact Analysis
BPA	Business Process Analysis
CCA	Continuous Control Assessment
CIO	Chief Information Officer
DCP	Division of Depositor and Consumer Protection
DIT	Division of Information Technology
DVD	Digital Versatile Disk
FDI	Federal Deposit Insurance
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISB	Infrastructure Services Branch
ISRM	Information Security Risk Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RADD	Regional Automated Document Distribution and Imaging System
RMS	Division of Risk Management Supervision
SP	Special Publication
SSN	Social Security Number
TLS	Transport Layer Security
USB	Universal Serial Bus

Part II

☆☆☆☆☆☆☆☆

FDIC Comments and OIG Evaluation

FDIC Comments and OIG Evaluation

The Director, RMS, and the CIO and Chief Privacy Officer provided a joint written response, dated June 15, 2020, to a draft of this report. The response is presented in its entirety on page II-2. FDIC management concurred with both of the report's recommendations and described corrective actions that the FDIC took to address the recommendations. Prior to finalizing the report, we confirmed that the FDIC's corrective actions were responsive, and we closed the recommendations. A summary of the FDIC's corrective actions is contained on page II-3.

FDIC Comments

Federal Deposit Insurance Corporation
550 17th Street NW, Washington D.C. 20429-990

Division of Risk Management Supervision
Chief Information Officer Organization

DATE: June 15, 2020

TO: Mark F. Mulholland
Assistant Inspector General for Information Technology Audits and Cyber

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

Sylvia W. Burns /**Signed/**
Chief Information Officer, Chief Privacy Officer & Director, DIT

SUBJECT:

SUBJECT: Management Response to the Draft Audit Report Entitled *Security Controls Over The Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System (Assignment No. 2018-021)*

Thank you for the opportunity to comment on the draft report prepared by the Office of Inspector General (OIG) on the Security Controls Over The Federal Deposit Insurance Corporation's (FDIC) Regional Automated Document Distribution and Imaging System (RADD) issued on May 29, 2020.

We are pleased that the OIG found the controls and practices over RADD were effective or partially effective in all eight of the security control areas assessed. In the draft report, the OIG recommended improvements in two security control areas that were not entirely consistent with FDIC policy requirements or not implemented in a manner consistent with relevant security guidance from the National Institute for Standards in Technology. FDIC management concurred with the two (2) OIG recommendations and completed actions to remediate both the Access Management and Audit controls identified as partially effective.

First, on September 24, 2019, the FDIC updated the RADD Audit Manual to improve the definition of audit roles, responsibilities, and procedures for reviewing and maintaining audit logs. Second, on August 26, 2019, the FDIC implemented a system modification to mitigate the access control finding relating to pre-indexed documents. The FDIC reviewed all 1.4 million documents accessed in 2019 and found no instances of unauthorized access.

We appreciate your staff's time and effort, and believe the FDIC has completed all actions necessary to address the OIG recommendations.

Summary of the FDIC's Corrective Actions

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC modified RADD to prevent users from accessing documents that had not yet been indexed.	August 26, 2019	$0	Yes	Closed
2	On August 30, 2019, the FDIC updated the RADD Audit Manual to improve the definition of audit roles, responsibilities, and procedures for reviewing and maintaining audit logs. On September 24, 2019, the FDIC subsequently clarified the audit manual to address the security, retention, and disposal of audit logs.	September 24, 2019	$0	Yes	Closed

[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 partially concurs or 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.