Security Configuration Management of the Windows Server Operating System

January 2019 **AUD-19-004**

Audit Report

Information Technology Audits and Cyber

☆☆☆☆☆☆☆☆

Integrity☆Independence☆Accuracy☆Objectivity☆Accountability

Executive Summary

Security Configuration Management of the Windows Server Operating System

At the start of 2018, the Federal Deposit Insurance Corporation (FDIC) had 2,166 servers on its network running the Microsoft Windows Server operating system. Because these servers store and process a significant volume of sensitive information and support mission-critical functions, a service disruption could impair the FDIC's ability to fulfill its mission of maintaining stability and public confidence in the nation's financial system. Ensuring the integrity, security, and reliability of the Windows Server operating system requires disciplined processes for managing the changes that occur to the system throughout its life cycle. Such changes include installing patches to address security vulnerabilities, applying software updates to improve functionality, and modifying configuration settings to improve security.

The Federal Information Security Modernization Act of 2014 requires Federal agencies to ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In addition, the National Institute of Standards and Technology (NIST) has issued guidance to help Federal agencies implement effective configuration management controls. Without effective configuration management, information systems may not operate properly, stop operating altogether, or become vulnerable to security threats.

The objective of the audit was to determine whether the FDIC established and implemented controls for managing changes to its Windows Server operating system that were consistent with Federal requirements and guidelines.

Results

The FDIC established various controls to manage changes to its Windows Server operating system that were consistent with Federal requirements and guidelines. Such controls included an approved baseline configuration for the operating system; a system to track, manage, and report system changes; and a Change Control Board to evaluate proposed changes.

We found that the FDIC, however, did not establish current policies and procedures for managing changes to the Windows Server operating system. Accordingly, we did not have sufficient criteria to fully assess the FDIC's implementation of configuration management controls. Current policies and procedures are important controls to ensure that employees and contractor personnel implement configuration management practices in a proper, consistent, and disciplined manner. The lack of

current policies and procedures limited the FDIC's ability to institutionalize roles and responsibilities, train staff on their duties, and effectively self-assess its configuration management practices.

We also found that the FDIC hired a contractor firm to assess certain security controls, including configuration management controls, for which the FDIC had also assigned the firm duties related to design and/or execution. According to NIST guidance, this arrangement impaired the firm's ability to conduct impartial security control assessments. The FDIC relies on the results of security control assessments to identify security weaknesses and inform key risk management decisions. A lack of impartiality could compromise the judgment of the assessor and the credibility of the assessment results.

In addition, we concluded that security control assessors did not perform testing, when appropriate, of certain security controls, including those intended to protect the Windows Server operating system. In these cases, assessors relied on written descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel. Without testing the implementation of these controls, assessors lacked a reliable basis to conclude on the effectiveness of the security controls. Inadequate FDIC oversight of security control assessments contributed to this weakness.

Further, we identified several inaccurate security control descriptions in the security plan for the Windows Server operating system. Many FDIC stakeholders rely on system security plans to make risk management decisions. For example, assessors use security plans to plan and conduct security control assessments. Inaccurate security control descriptions could result in erroneous control testing, or untested controls. In addition, the FDIC's authorizing official uses the information in security plans to authorize systems to operate. Inaccurate security control descriptions can negatively affect the integrity of these decisions.

Recommendations

Our report includes eight recommendations addressed to the Chief Information Officer (CIO) that, collectively, intend to ensure (a) IT policies and procedures remain current and that personnel responsible for their implementation receive proper training; (b) security control assessments are performed by sufficiently independent entities; (c) oversight of security control assessments is sufficient and documented; and (d) system security plans remain accurate.

In a written response to the report, the CIO Organization concurred with all eight recommendations. The CIO Organization completed actions to address two of the recommendations and plans to complete actions to address the remaining six recommendations by November 29, 2019.

Contents

Background **2**

Roles and Responsibilities 4

The FDIC's Change Management System 5

Audit Results **6**

Outdated Policies and Procedures 6

Security Control Assessments Lacked Independence 10

Inadequate Depth and Coverage of Assessments 15

Inaccurate Security Plan Information 19

FDIC Comments and OIG Evaluation **21**

Appendices

1. Objective, Scope, and Methodology 22
2. Glossary 25
3. Acronyms and Abbreviations 28
4. Untested Security Controls 29
5. FDIC Comments 30
6. Summary of the FDIC's Corrective Actions 35

Table

Control Assessments Without Testing 16

Figures

1. Phases of Configuration Management 3
2. Organizational Structure of the CIO Organization 4

January 16, 2019

Howard G. Whyte
Chief Information Officer and Chief Privacy Officer

Subject ***Security Configuration Management of the Windows Server Operating System***

As of January 8, 2018, the Federal Deposit Insurance Corporation (FDIC) had 2,166 servers on its network running the Microsoft Windows Server operating system. These servers store and process a significant volume of information, including sensitive personally identifiable information,[1] confidential bank examination reports and supervisory ratings, lists of banks scheduled for closing, and plans for the resolution of systemically important financial institutions. Windows servers also support mission-critical functions, such as processing deposit insurance assessments for financial institutions, tracking financial claims against failed banks in receivership, and managing human resources information about FDIC employees. Accordingly, a service disruption involving the Windows Server operating system could impair the FDIC's ability to fulfill its mission to maintain stability and public confidence in the nation's financial system.

Ensuring the integrity, security, and reliability of any information system requires disciplined processes for managing the changes that occur to the system during its life cycle. Such changes include installing software patches to address security vulnerabilities, applying software updates to improve system performance and functionality, and modifying configuration settings to strengthen security. Managing these types of changes is referred to as configuration management. Configuration management refers to the collection of activities focused on establishing and maintaining the integrity of IT products and systems. An organization fosters system integrity by controlling the processes for initializing, changing, and monitoring the configurations of those IT products and systems throughout the system development life cycle. Without effective configuration management, the FDIC's information systems may not operate properly, stop operating altogether, or become vulnerable to security threats.

The objective of our audit was to determine whether the FDIC established and implemented controls for managing changes to its Windows Server operating system that were consistent with Federal requirements and guidelines. We conducted this performance audit in accordance with generally accepted government auditing

[1] Appendix 2, *Glossary*, defines terms that are underlined when first used in this report.

standards. Appendix 1 of this report provides additional details about our objective, scope, and methodology; Appendix 2 contains a glossary of terms; Appendix 3 contains a list of acronyms and abbreviations; Appendix 4 identifies security controls for which the FDIC did not perform testing; and Appendix 5 and Appendix 6 contain the FDIC's comments on this report and a summary of the Corporation's corrective actions.

Background

The Federal Information Security Modernization Act of 2014 (FISMA 2014)[2] requires Federal agencies, including the FDIC, to develop, document, and implement an agency-wide information security program to protect their information and information systems. The statute requires that such security programs include policies and procedures to ensure agencies comply with their "minimally acceptable system configuration requirements." Agencies develop and record these configuration requirements in a document or repository called a "baseline configuration." A baseline configuration serves as a set of specifications for a system and can only be changed through a formal change control process. Agencies use baseline configurations as a frame of reference to assess their systems for compliance with configuration requirements and to help manage future builds, releases, and/or changes. Baseline configurations therefore serve as an important control for securing and managing changes to information systems.

FISMA 2014 directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist Federal agencies in defining security requirements for their information systems.[3] In March 2006, NIST issued *Minimum Security Requirements for Federal Information and Information Systems* (FIPS Publication 200). FIPS Publication 200 is a mandatory standard that defines minimum security requirements for Federal information and information systems in seventeen security-related areas, including configuration management. According to FIPS Publication 200, Federal agencies must:

> (i) *Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and*

[2] Public Law (P.L.) No. 113-283.
[3] NIST establishes and communicates required security standards in Federal Information Processing Standard (FIPS) Publications and recommended (i.e., nonbinding) guidelines in its Special Publications (SP). NIST publications provide Federal agencies with a framework for developing appropriate security controls for their information and information systems.

(ii) *Establish and enforce security configuration settings for information technology products employed in organizational information systems.*

To help agencies address the security requirements contained in FIPS Publication 200, in December 2006, NIST issued a revision to *Recommended Security Controls for Federal Information Systems* (SP 800-53, Revision 1).[4] NIST SP 800-53 contains guidelines to help agencies select and specify security controls (including configuration management controls) to protect their information systems. Further, in August 2011, NIST issued a *Guide for Security-Focused Configuration Management of Information Systems* (SP 800-128) which supplements the earlier NIST SP 800-53 by providing agencies with detailed guidance for implementing their configuration management controls.

Figure 1: Phases of Configuration Management

Source: Office of Inspector General (OIG) analysis of NIST SP 800-128

As reflected in Figure 1, NIST SP 800-128 describes the four phases of configuration management. The *Planning* phase (#1) involves developing configuration management policies and procedures that address configuration management plans, configuration control boards, configuration control processes, tools, and technologies, and baseline configurations. The second phase, *Identifying and Implementing Configurations* (#2), involves developing, approving, and implementing baseline configurations for information systems.

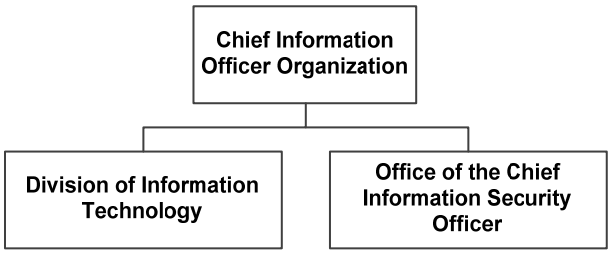
The third phase, *Controlling Configuration Changes* (#3), involves maintaining secure, approved baseline configurations for each information system. During this phase, the agency identifies, proposes, reviews, analyzes, tests, and approves system changes prior to implementation. To support these activities, NIST recommends that agencies implement configuration management policies, procedures, automated tools, and other controls to prevent unauthorized and/or undocumented changes. The fourth phase, *Monitoring* (#4), involves validating that information systems adhere to established policies, procedures, and approved baseline configurations. Effective monitoring can identify unauthorized system components, misconfigurations, vulnerabilities, and needed changes that could expose agencies to increased risk if left unaddressed.

[4] NIST issued three updates to SP 800-53 since Revision 1. NIST issued the current version (Revision 4) in April 2013.

Roles and Responsibilities

Within the FDIC, the Chief Information Officer (CIO) Organization has strategic responsibility for information technology (IT) governance, investments, program management, and information security. The CIO Organization is led by the CIO, who also serves as the FDIC's Chief Privacy Officer. The CIO reports directly to the Chairman of the FDIC's Board of Directors. As depicted in Figure 2, two separate component organizations report to the CIO: the Division of Information Technology (DIT) and the Office of the Chief Information Security Officer (CISO). DIT has primary responsibility for the day-to-day operational support and management of the FDIC's information systems and IT infrastructure. The Office of the CISO is responsible for fulfilling the CIO's responsibilities under FISMA 2014—most notably, the planning, development, and implementation of an agency-wide information security program.

Figure 2: Organizational Structure of the CIO Organization



Source: OIG analysis of the CIO Organization's Web site.

DIT and the Office of the CISO play important roles in ensuring the proper configuration of the FDIC's information systems. DIT's Infrastructure Services Branch (ISB) has primary responsibility for establishing and maintaining baseline configurations for the FDIC's information systems, including the Windows Server operating system. ISB personnel also track, manage, test, and implement software changes to information systems. In addition, the Deputy Director for ISB serves as the Chairperson of DIT's Change Control Board—a body consisting of the Deputy Director and eight voting members from different program areas within the CIO Organization charged with deciding whether to approve proposed changes to information systems.[5]

The Office of the CISO manages the Vulnerability Management Program which identifies, tracks, and reports vulnerabilities affecting the security of FDIC information systems. In operating this program, Blue Canopy LLP (Blue Canopy), a firm engaged by the FDIC to provide information security services, performs regular scans of FDIC information systems to identify configuration-related vulnerabilities. The Office of the CISO provides the results of these scans to various

[5] The eight voting members are from the following CIO Organization program areas: Operations, Engineering, Help Desk/Client Services, Delivery Management Branch, Enterprise Information Management, Development and Engineering Support Section, Security Protection Engineering Section, and Software Engineering Support and Web Technologies.

CIO Organization stakeholders who use the information to evaluate and remediate vulnerabilities and monitor the overall security posture of information systems.

The Office of the CISO also manages the Continuous Controls Assessment (CCA) Program. In implementing this program, Blue Canopy assesses security controls to determine their effectiveness (i.e., whether implemented correctly). Blue Canopy documents the results of these assessments in CCA Reports. The CIO Organization uses the information in CCA Reports to identify and address weaknesses affecting the security of information systems and to inform key risk management decisions, such as authorizing the operation of information systems.[6]

The FDIC's Change Management System

In October 2016, DIT began using its automated change management system, ServiceNow, to track, manage, and report information about proposed and approved configuration changes to the FDIC's information systems. ServiceNow replaced DIT's legacy change management system of record, Remedy. ServiceNow tracks such information as:

- Who requested the change;
- The status/phase of the change;
- The planned and actual start and end dates for the change;
- The information systems affected by the change;
- A description of, and reason for, the change;
- A description and results of security impact testing/analysis performed; and
- Change Control Board member voting results.

During 2016, CIO Organization personnel implemented 53 changes to the approved baseline configuration for the Windows Server operating system. Such changes included restricting the use of removable media, increasing the storage limits of Windows Server log files, and modifying access privileges for Windows administrator accounts. In addition to baseline configuration changes, the Microsoft Corporation, the vendor for the Windows Server operating system, recommended that its customers running the 2008 and 2012 versions of the system[7] install 286 security patches during calendar year 2016.[8] The CIO Organization needed to assess each

[6] Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016) (OMB Circular A-130) requires Federal agencies to authorize their information systems to operate. A senior management official (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.

[7] The FDIC primarily used the 2008 and 2012 versions of the Windows Server operating system. The FDIC operated a limited number of servers running Windows Server 2003 until late 2016. Because the FDIC retired these servers before we began our audit, we excluded them from our scope.

[8] Based on our analysis of patch information on the Microsoft Corporation's website.

of these patches to determine whether they should be installed in the FDIC's IT environment.

Audit Results

The FDIC established various controls to manage changes to its Windows Server operating system that were consistent with Federal requirements and guidelines. Such controls included an approved baseline configuration, change management tools and systems, and a Change Control Board. However, the FDIC did not maintain updated policies and procedures for managing changes to the system. Without current FDIC policies and procedures, we did not have sufficient criteria to assess the FDIC's configuration management practices. Accordingly, we could not fully assess the FDIC's implementation of configuration management controls.

We developed findings with respect to (i) outdated policies and procedures for managing changes to the Windows Server operating system, (ii) a lack of independence of the organization that conducted security control assessments of the system, (iii) inadequate depth and coverage of security assessments, and (iv) inaccurate information in the system security plan.

Outdated Policies and Procedures

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* states that policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal government. According to FIPS Publication 200, agencies must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in the standard and must ensure their effective implementation.

The fourth revision to NIST's guidance on *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53, Revision 4), recommends that agencies establish policies and procedures for managing the configuration of their information systems. According to the NIST publication, organizations should review and update these policies and procedures. In addition, the Government Accountability Office's *Standards for Internal Control in the Federal Government* and FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*

(dated April 16, 2012),[9] emphasize the importance of policies and procedures as critical components of an effective internal control system.

The implementation of ServiceNow introduced new workflow processes for collecting, organizing, maintaining, and reporting information related to system changes. At the time ServiceNow was implemented in October 2016, DIT's *Change Management Process* document, Version 1.3 (August 2014), defined procedures for planning, coordinating, and implementing configuration changes to the FDIC's information systems.[10] DIT considered compliance with this document to be critical to controlling changes and preserving the integrity and service quality of the FDIC's IT environments. However, DIT did not update its *Change Management Process* procedures document to reflect the implementation of ServiceNow. The document identified Remedy as the FDIC's change management system of record and contained detailed instructions for using Remedy workflow processes to manage, track, and review changes.

FDIC Did Not Prioritize Policies and Procedures

The procurement of ServiceNow was approved by the former Deputy Director for ISB in June 2015, more than a year before its implementation. Prior to the implementation of ServiceNow in October 2016, DIT had ample opportunity to establish policies and procedures governing its use. According to the CIO, the FDIC did not update the *Change Management Process* document—a key document instructing DIT personnel how to perform their configuration management duties—to reflect the use of ServiceNow until August 2017, almost a year after DIT began using the system to manage configuration changes to the FDIC's information systems.

DIT's Deputy Director for ISB informed us that he considered the retirement of Remedy as a high priority in 2016 because the system presented both operational and security risks. The Deputy Director explained that the FDIC used a version of Remedy for which the vendor stopped providing technical support, including software patches, more than 2 years earlier (March 2014). In addition, the version of Remedy that the FDIC used ran on the Windows Server 2003 operating system, for which the Microsoft Corporation discontinued extended support in July 2015.

In our prior audits, we identified similar instances in which the CIO Organization implemented new or modified processes or programs without establishing or updating corresponding policies and procedures.

[9] In October 2018, the FDIC superseded this Circular, replacing it with FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program.*

[10] The CIO Organization issued the following additional configuration management-related policies and procedures: Policy 16-005, *Policy on Secure Baseline Configuration Guides* (December 9, 2016); Policy 15-003, *Policy on Security Patch Management* (October 2, 2015); *Secure Baseline Configurations Program Process and Procedures* Version 3.0 (June 15, 2016); Work Instruction-607, *Microsoft Security Patch Deployment*, Release 2.0 (undated); *Security Patch Testing and Deployment Procedure – Microsoft Windows*, Version 1.6 (May 21, 2015).

- In June 2017, we reported that the CIO Organization had begun requiring employees and contractor personnel to use identity credentials known as personal identity verification (PIV) cards to access the network.[11] However, the CIO Organization did not establish policies and procedures to govern network access using PIV cards. In our report, we recommended that the CIO establish such policies and procedures; this recommendation has since been closed.
- In September 2017, we reported that the FDIC had not established policies and procedures before it began using the data loss prevention tool in the employee and contractor pre-exit process.[12] We recommended that the Director, Division of Administration (DOA), work with the CIO to establish appropriate policy in this area. At the close of this present audit, the Director, DOA, and CIO had not yet completed actions to address our recommendation.

Interim OIG Reporting During Audit Fieldwork

In June 2017, we notified the CIO Organization that its configuration management policies and procedures did not reflect current practices and that we had observed inconsistent change management records in ServiceNow related to the Windows Server operating system. CIO Organization staff responded that they were revising the *Change Management Process* document and certain other configuration management procedures to address the concerns we raised.

In our FISMA report issued in October 2017,[13] we reported that DIT had not updated the *Change Management Process* document to address the implementation of ServiceNow. We also reported that ServiceNow included both incomplete and inconsistent change management records. For example, ServiceNow (a) did not consistently contain evidence of Change Control Board approvals of changes, as appropriate; (b) did not consistently reflect the correct category of changes; and (c) included conflicting information regarding the status of changes. We recommended that the CIO update the *Change Management Process* document to track and manage changes to the FDIC's information systems.

In a written response to this FISMA report, the CIO stated that the FDIC updated the *Change Management Process* document in August 2017 to reflect the use of ServiceNow. The CIO also stated that the CIO Organization continued working to create a Change Management Policy, an ISB Change Management Procedure, and a new work instruction to explain the use of ServiceNow by DIT staff to implement

[11] See OIG Report, *Follow-on Audit of the FDIC's Identity, Credential, and Access Management (ICAM) Program* (June 2017).
[12] See OIG Report, *Controls over Separating Personnel's Access to Sensitive Information* (September 2017).
[13] See OIG Report, *Audit of the FDIC's Information Security Program—2017* (October 2017). We conducted fieldwork for this audit from April through September 2017.

the change management process. Such policies and procedures would encompass the Windows Server operating system. On July 26, 2018, subsequent to the close of the present audit, CIO Organization management provided the OIG with a corrective action closure (CAC) package to address our recommendation from the FISMA report. The OIG completed its review of the CAC package in September 2018 and determined that it was responsive to the recommendation.

Limited Ability to Assess Controls

We judgmentally selected for detailed review 20 security patches recommended by the Microsoft Corporation and 10 changes to the Windows Server operating system baseline configuration. We confirmed that the FDIC applied these patches and baseline configuration updates. However, we could not assess whether the CIO Organization effectively managed these changes, because it had not established current policies and procedures that we could use as criteria to conduct such an assessment.

We also observed that DIT personnel did not consistently record in ServiceNow information related to patches and changes to the baseline configuration. For example, DIT did not record in ServiceNow 7 of the 20 security patches we reviewed. In addition, DIT did not record its verification that baseline configuration changes were appropriately implemented for all 10 changes we reviewed. Further, DIT did not maintain records documenting when it had fully deployed security patches in a readily available format. As a result, we could not determine whether DIT met the CIO Organization's established patching schedule.[14]

Up-to-date policies and procedures are an important control for ensuring that employees and contractor personnel implement configuration management practices in a proper, consistent, and disciplined manner. The lack of current policies and procedures limited the FDIC's ability to institutionalize and communicate roles and responsibilities and train staff on their duties. Without current policies and procedures, DIT was dependent on the knowledge and experience of key staff, which exposed the FDIC to operational risk associated with workforce staffing changes. For example, the departure of key staff increased the risk that changes will not be managed consistent with management's expectations.

Further, NIST recommends that agencies conduct self-assessments to determine whether configuration management controls function as intended. Absent current

[14] The CIO Organization's *Policy on Security Patch Management* (CIO Organization Policy 15-003) requires vendor-released patches to be installed within the timeframes established in the *CIO Organization Security Patching Schedule*. This schedule states that DIT must install security patches for the Windows Server operating system within a specific timeframe after notification from the Office of the CISO that the system needs a patch.

policies and procedures and consistent and complete information in ServiceNow, the FDIC's ability to effectively conduct such self-assessments was limited.

Recommendations

We recommend that the CIO:

1. Train personnel on their updated roles and responsibilities as defined in the revised configuration management policies and procedures.

   As noted in our report, in response to a recommendation in our FISMA report issued in 2017, the CIO agreed to update the CIO Organization's configuration management policies and procedures.

2. Establish and implement controls to ensure that CIO Organization policies and procedures are established before deploying new or modified IT processes or programs.

Security Control Assessments Lacked Independence

FISMA 2014 requires Federal agencies to test and evaluate their information security controls periodically to ensure they are effectively implemented. According to NIST, such assessments are the principal vehicle used by agencies to verify that security controls meet their stated goals and objectives.[15] NIST recommends that agencies use independent assessors to conduct such work, which NIST defines as any individual or group capable of conducting an impartial assessment. Impartial means that security control assessors are free from any perceived or actual conflicts of interest with respect to any of the following functions: the development, operation, and/or management of the information system or the determination of security control effectiveness through assessment activities. A lack of impartiality could compromise the judgment of the assessor and the credibility of the assessment results. Therefore, according to NIST guidance, assessors should not assess the effectiveness of their own work.[16]

According to NIST SP 800-53A, agency authorizing officials—management officials responsible for authorizing Federal information systems to operate—have responsibility for determining the level of independence required for assessors.

[15] NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (December 2014).
[16] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

Such determinations are based principally on the security category[17] of the information system to be assessed. NIST recommends that agencies use independent assessors to assess the effectiveness of security controls protecting information systems designated either "moderate" or "high" potential impact.[18] Agency authorizing officials may exercise discretion in determining whether to use independent assessors for systems designated "low" impact. The FDIC has designated the Windows Server operating system as having "moderate" potential impact.

NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach,* SP 800-37, Revision 1, (February 2010) states that assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of security assessment results; and (iii) ensuring that authorizing officials receive the most objective information possible to make informed, risk-based authorization decisions.

We reviewed the FDIC's contracts with Blue Canopy and found that they tasked the firm with duties related to the design and execution of configuration management-related security controls. For example, the contracts tasked Blue Canopy with the following duties:

- Regularly scan for and track vulnerabilities on information systems;
- Create, maintain, and perform a process for analyzing the security impacts of proposed information system changes;
- Work with FDIC information security staff to produce, maintain, and update security baseline configurations;
- Serve as a backup for change control decisions when the DIT Information Security Manager (ISM)[19] is unavailable.

In addition, the FDIC tasked Blue Canopy under the CCA Program with assessing the effectiveness of security controls related to each of the foregoing duties. Tasking Blue Canopy with assessing the effectiveness of its own work limited the firm's independence which, according to NIST guidance, impaired the firm's ability to conduct an impartial assessment.

[17] NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), requires agencies to categorize their information systems as high, moderate, or low. This category reflects the potential impact to the agency should certain events occur which jeopardize the information and information systems needed to accomplish the agency's assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
[18] NIST's *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management* (June 2014).
[19] ISMs are employees tasked with providing a security focus within their respective divisions and offices and with working to educate employees and contractors on security risks. ISMs are also required to assess the level of security in applications and information service providers; ensure that security requirements are addressed in new or enhanced systems; and promote compliance with FDIC security policies and procedures.

Representatives of Blue Canopy stated that, notwithstanding its contractual duties described above, the firm did not design or implement configuration management controls. The representatives explained that the firm believed that its role in developing such controls was as a consultant to FDIC system stakeholders. In addition, with respect to the fourth bullet above, Blue Canopy representatives felt that its role was to provide support for the ISM, including collection of documentation for the ISM's review. The representatives asserted that the firm did not make or approve change control decisions on behalf of the ISM.

Our review of the FDIC's contracts with Blue Canopy also found that the FDIC tasked Blue Canopy to assist system owners and other stakeholders in the remediation of security weaknesses that the firm identifies, and validate the adequacy of corrective actions taken to address those weaknesses. Further, the FDIC tasked Blue Canopy within contracts to perform the following duties:

- Operate the Computer Security Incident Response Team, which includes incident detection and response activities;
- Operate the Security Operations Center, which includes monitoring for network intrusions, investigating security incidents, and reporting investigative activities;
- Design and implement updates to the information security continuous monitoring program; and
- Process requests for elevated access privileges in FDIC systems.

The FDIC's contracts with Blue Canopy required that the firm not only conduct these duties, but also assess their effectiveness as part of the CCA Program.

Lack of Independence Impacted Credibility of Security Control Assessments

Our review of selected security controls revealed circumstances that could create, at least, a perception that the lack of independence described above influenced the judgment of assessors in planning and executing security control assessments.

As stated earlier, Blue Canopy regularly scans for and tracks weaknesses identified on the FDIC's information systems as part of the Vulnerability Management Program.[20] NIST SP 800-53, Revision 4, refers to this configuration management-related control as *Vulnerability Scanning*.[21] The FDIC tasked Blue Canopy under the CCA Program with assessing the effectiveness of *Vulnerability Scanning*. Since it

[20] NIST SP 800-123, *Guide to General Server Security* (July 2008), recommends that agencies conduct vulnerability scanning to validate that operating systems and server software are up-to-date on security patches and software versions.
[21] The CCA Program has categorized this control as a "critical control," meaning that it requires continuous monitoring based on trends from previous assessments and audits, as well as its high impact on the FDIC mission, critical assets, sensitive data and/or other systems across the enterprise. According to the FDIC's *CCA Methodology* document (February 2017), 11 of the 177 (6 percent) controls in NIST SP 800-53, Revision 4, covered by the CCA Program have been categorized as a "critical control."

began assessing this control in June 2010, Blue Canopy has not identified and reported to FDIC management any weaknesses pertaining to its implementation of *Vulnerability Scanning*.[22] However, in 2016 and 2017, we identified weaknesses that limited the effectiveness of this control. These weaknesses existed during the period in which Blue Canopy was responsible for assessing *Vulnerability Scanning*.

In our FISMA report issued in 2016,[23] we reported that more than 900 (i.e., one-third) of the production Windows servers on the FDIC's network were not subjected to regular vulnerability scans. Further, in our FISMA report issued in 2017, we noted instances in which the FDIC did not subject network IT devices to a "credentialed" scan—a thorough type of scan recommended by NIST that requires logging into the IT device to inspect for vulnerabilities. We reported that these weaknesses diminished the FDIC's assurance that it would sufficiently detect and address network vulnerabilities in a timely manner.

We reviewed Blue Canopy's CCA Report (dated December 2016) and noted that the firm's assessment of *Vulnerability Scanning* sought to, among other things, determine whether Blue Canopy performed scans on at least a monthly basis. The CCA Report stated "occasionally, one or more scans may not be completed before the deadline for one reason or another." However, the CCA Report did not quantify how many scans were not completed on time, or how frequently this occurred. The CCA Report also stated that the FDIC's vulnerability scanning tool "lists all devices that have not been scanned for 60 days or more." However, the report did not quantify how many or what types of systems were not scanned on at least a monthly basis, or how much time had elapsed between scans.

Representatives of Blue Canopy asserted that the *Vulnerability Scanning* control described in NIST SP 800-53, Revision 4, did not require that all IT assets be subject to a successful scan and it did not specify a number or percentage of IT assets as a threshold for failing the *Vulnerability Scanning* control. According to the Blue Canopy representatives, the *Vulnerability Scanning* issues in the CCA Report were identified through its review of the FDIC's vulnerability scanning procedures. Blue Canopy did not conduct control testing in this area. Blue Canopy representatives added that the firm did not compare the IT asset inventory to scan results, because it was not required. Blue Canopy reported that the *Vulnerability Scanning* control was effectively implemented by marking the assessment step as a "Pass." As a result, the firm did not create any POA&Ms related to the *Vulnerability Scanning* weaknesses referenced in its CCA Report.

[22] Blue Canopy records weaknesses it identifies during security control assessments in Plans of Action and Milestones (POA&Ms). The FDIC uses POA&Ms to track, address, and report progress in remediating security weaknesses affecting its information systems. Blue Canopy recorded one weakness in a POA&M associated with *Vulnerability Scanning*, but the weakness was unrelated to the firm's implementation of the control.

[23] See OIG Report, *Audit of the FDIC's Information Security Program—2016* (November 2016).

In light of our findings related to *Vulnerability Scanning*, we expanded our review of Blue Canopy's assessments to include two additional security controls that the firm implements: *Incident Handling* and *Incident Monitoring*.[24] *Incident Handling* includes the preparation, detection, analysis, containment, eradication, and recovery activities for information security incidents. *Incident Monitoring* consists of tracking and documenting such incidents. To implement these two controls, Blue Canopy staffs and operates the FDIC's Computer Security Incident Response Team and Security Operations Center. At the close of our fieldwork, Blue Canopy had not reported any weaknesses under the CCA Program related to the firm's implementation of *Incident Handling* or *Incident Monitoring* since it began assessing these controls in June 2010.[25]

However, our office issued several reports between 2016 and 2018[26] describing weaknesses in the FDIC's handling and monitoring of information security incidents. Collectively, the OIG made 12 recommendations to the FDIC in these reports that were intended to improve the FDIC's handling and monitoring of incidents. In written responses to these reports, FDIC officials described planned corrective actions to address our recommendations. As of the date of this report, the FDIC had completed corrective actions to address all of these recommendations.

Inadequate Controls for Ensuring Assessor Independence

The FDIC's policies, procedures, and guidance do not define an approach for ensuring assessor independence. Representatives of the Office of the CISO informed us that they consider a Blue Canopy employee assessing a given control to be independent if the individual performing the assessment did not also design or implement that control. However, this approach does not mitigate the risks of an organizational conflict of interest. Such conflicts can arise when the FDIC tasks a firm to evaluate the same services it provides, or to make recommendations concerning programs that could affect the firm's financial interest. Such scenarios compromise both the objectivity of the assessor's advice and the value of the FDIC's expenditures for such services. For example, Blue Canopy may be influenced to refrain from reporting a weakness related to a control that the firm has designed or implemented because doing so might reflect negatively on the firm, or expose the firm to increased expenses to correct the weakness.

[24] *Incident Handling* and *Incident Monitoring* are 2 of 10 Incident Response-related controls recommended by NIST SP 800-53, Revision 4. The remaining eight controls are *Incident Response Policies and Procedures*, *Incident Response Training*, *Incident Response Testing*, *Incident Reporting*, *Incident Response Assistance*, *Incident Response Plan*, *Information Spillage Response*, and *Integrated Information Security Analysis Team*. The scope of our audit did not include assessing the extent to which Blue Canopy identified weaknesses for these eight controls.

[25] Blue Canopy recorded one weakness associated with *Incident Handling* in a POA&M, but the identified weakness was unrelated to the firm's implementation of the control.

[26] See OIG Reports, *The FDIC's Process for Identifying and Reporting Major Information Security Incidents* (July 2016, Revised February 2017), *The FDIC's Processes for Responding to Breaches of Personally Identifiable Information* (September 2017); and *The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches* (April 2018).

The FDIC needs to define in its policies, procedures, or guidance the required level of independence for its security control assessments. This information will serve to mitigate apparent and actual conflicts of interest and promote the credibility of assessment results.

Recommendation

We recommend that the CIO:

3. Establish requirements to ensure the independence of security control assessors.

Inadequate Depth and Coverage of Assessments

NIST guidance on *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, SP 800-53A, Revision 4, defines procedures to guide agencies in conducting effective security control assessments. This NIST guidance allows agencies to customize these procedures and determine the appropriate level of depth and coverage to use in security control assessments.[27] NIST SP 800-53A identifies three principle methods of executing assessment procedures:

1) *Examining* security information and activities (for example, policies, procedures, plans, architectural designs, backup operations, and network monitoring);
2) *Interviewing* individuals or groups, such as system owners and network administrators; and
3) *Testing* security controls.

According to NIST, agencies should consider various factors specific to the agency's information systems and the environments in which they operate in determining the assessment procedures to be performed and their level of depth and coverage. Such factors include the level of assurance needed from the assessment;[28] known threat and vulnerability information; and the agency's risk tolerance.

The FDIC relies on the results of security control assessments to support a number of important risk management activities. These include identifying security weaknesses in information systems and the IT environment; prioritizing risk mitigation activities; confirming the resolution of known security weaknesses; informing security authorization decisions; and supporting resource allocation

[27] Depth refers to the rigor and level of detail involved in executing assessment procedures. Coverage refers to the scope or breadth of the assessment procedures.
[28] For example, information systems categorized as high or moderate impact generally require a greater level of depth and coverage than systems categorized as low impact

decisions. For these reasons, the FDIC must ensure that it conducts security control assessments at an appropriate level of depth and coverage.

We reviewed the procedures performed by Blue Canopy to assess certain configuration management-related control activities for the Windows Server operating system. We concluded that security control assessors did not perform testing, when appropriate, for certain control activities. Our review of assessment procedures for 30 judgmentally-selected security control activities described in a CCA Report finalized in December 2016 identified three instances in which assessors did not perform any testing and only examined narrative descriptions of the control activities in the system's security plan. Without testing, assessors did not have a basis for concluding on the effectiveness of the security control activities. The Table below describes each of the three control activities, Blue Canopy's assessment conclusions, and the testing needed to support a conclusion regarding effectiveness.

Table: Control Assessments Without Testing

NIST-Recommended Control Activity	Blue Canopy Assessment Conclusion	Testing Needed to Assess Effectiveness
Agency retains records of changes to information systems for the agency's defined time period.	Pass: "[The FDIC] retains records of configuration-controlled changes to the information system for at least the last generation."	Verification that the FDIC retained records for specific changes to the system in accordance with the FDIC's records retention policy.
Agency audits and reviews activities associated with changes to information systems.	Pass: "[The FDIC] audits and reviews activities associated with configuration-controlled changes to the information system."	Examination of records supporting that the FDIC has conducted audits or reviews of change management activities related to the system.
Agency installs security patches within agency-defined time period of the release of the patch.	Pass: "[The FDIC] installs security-relevant software and firmware updates within the established timeframes (in accordance with the FDIC Policy 15-003 on Security Patch Management) of the release of the updates."	Inspection of records that demonstrate the FDIC has applied security patches to servers within the timeframes established in CIO Organization policy.

Source: OIG review of the Windows Server operating system CCA Report for December 2016
Pass = A conclusion of "Pass" means that the assessors concluded that the security control activity was effective.

In June 2017, we notified staff in the Office of the CISO of the three security control activities for which assessors did not perform testing. They agreed that the procedures performed were not adequate. The FDIC subsequently requested that Blue Canopy assess these control activities a second time and review the firm's prior-year assessments of these control activities to determine whether similar shortcomings existed. Based on the reassessment work, Blue Canopy determined that the three control activities were effective and that previous assessments of these control activities were adequate, and the Office of the CISO concurred.

We learned through subsequent discussions with Office of the CISO staff that Blue Canopy billed the FDIC for the reassessment work described above. The FDIC's contract with Blue Canopy states that, with certain exceptions, the firm shall complete rework at no charge to the FDIC. We brought this concern to the attention of Office of CISO staff who subsequently took action to recoup the cost of the rework ($1,080) from Blue Canopy. Accordingly, we designated the $1,080 amount as questioned costs.

Untested Security Controls

Based on the concerns we identified regarding the depth and coverage of security control assessments for the Windows Server operating system, we expanded our audit procedures to include five CCA Reports covering two additional information systems and certain common controls.[29] Blue Canopy completed these reports in 2016 and 2017. We found that the concerns described above were not limited to the Windows Server operating system.

Appendix 4 identifies 18 additional security control activities for which we concluded Blue Canopy assessors should have conducted testing. These control activities included such things as updating and testing IT contingency plans, performing system backups, and scanning for and remediating security vulnerabilities. Assessors concluded that these control activities were effective based only on their examination of documentation that described the control activity's design and/or interviews of FDIC or other Blue Canopy personnel.

Further, our expanded procedures identified one NIST-recommended security control activity that, despite being targeted for assessment, was not assessed at all. NIST SP 800-53, Revision 4, recommends that agencies configure their information systems to allow for privileged access when conducting vulnerability scans (a process known as credentialed scanning). Instead of determining whether the FDIC's information systems are configured to allow credentialed scans, Blue Canopy assessed how the FDIC granted and provided user access in its vulnerability scanning tool. As a result, Blue Canopy did not have adequate evidence on which to base its conclusion that the FDIC effectively implemented this NIST-recommended security control activity.

As previously mentioned, our FISMA audit conducted in 2017 found instances in which the FDIC did not subject network IT devices to credentialed scans. We recommended that the CIO review and enhance the FDIC's vulnerability scanning process accordingly. At the close of this audit, the FDIC had not completed corrective actions to address this recommendation. Without credentialed scans, the

[29] Appendix 1 describes our methodology in selecting CCA Reports for review.

FDIC lacks complete information about the security posture of IT devices connected to the network.

Need for Formal Review of CCA Reports

After completing security control assessments, Blue Canopy submits draft CCA Reports to the CCA Program Manager for review.[30] As a matter of practice, the CCA Program Manager provides these draft CCA Reports to various stakeholders, such as system owners and security professionals, and formally accepts the reports.

The CIO Organization did not develop written procedures for reviewing CCA Reports to ensure they are consistent with applicable requirements in contractual agreements between Blue Canopy and the FDIC. In addition, the FDIC does not require the CCA Program Manager to document the results of CCA Report reviews. The CCA Program Manager informed us that Blue Canopy completes a quality assurance checklist before submitting each CCA Report to the FDIC; however the CCA Program Manager does not confirm whether Blue Canopy actually performs the actions described on the checklist. During 2017, the FDIC paid Blue Canopy approximately $2.4 million for security control assessment work performed under the CCA Program. In light of the critical role these reports play in the security of the FDIC's information systems, and the amount of resources invested in this area, the FDIC should implement a formal review and approval process for CCA Reports. Such a process would help ensure appropriate scrutiny of CCA reports and help to identify areas where greater depth and coverage of security control assessment work is needed.

Recommendations

We recommend that the CIO:

4. Establish and implement procedures to ensure that contractor-submitted CCA Reports are reviewed for consistency with applicable requirements in contractual agreements and that such reviews are documented.

5. Require that CIO Organization management ensure the sufficiency of CCA Report reviews and provide feedback when review activities are deemed insufficient.

6. Recover $1,080 in questioned costs paid to Blue Canopy.

[30] The CCA Program Manager serves as the FDIC's Technical Monitor for security control assessment activities performed under the contract with Blue Canopy. FDIC Circular 3700.16, *FDIC Acquisition Policy Manual*, defines roles and responsibilities for overseeing the work of contractors, such as Blue Canopy. According to the Circular, Technical Monitors are responsible for assisting in the oversight of contractor performance and the review and acceptance of contractor work products.

Inaccurate Security Plan Information

OMB Circular No. A-130 requires Federal agencies to develop and maintain security plans for their information systems. This Circular states that security plans must document the security controls in the system and describe the implementation of those controls. In addition, NIST's *Guide for Developing Security Plans for Federal Information Systems*, SP 800-18, Revision 1 (February 2016), explains that the purpose of the security plan is to provide an overview of the security requirements for the information system and to describe the security controls in place, or planned, for meeting those requirements. NIST SP 800-18 states that the security plan is a "living document" that requires periodic review and updating to reflect the current state of the system.

We reviewed the descriptions of configuration management controls in the security plan for the Windows Server operating system as of June 20, 2017 and identified the following three deficiencies:

- *Flaw Remediation.* This control description stated that the FDIC utilized the Microsoft System Center Configuration Manager tool to deploy and verify all patches and the Shavlik tool to scan for missing patches. However, as of August 2015, the FDIC no longer used the tools for these purposes.
- *Configuration Management Plan.* This security control description stated that the *Change Management Process* document, Version 1.3, is part of the configuration management plan for the system. However, the *Change Management Process* document omitted specifications recommended by NIST for configuration management plans, such as the identification of the specific system components subject to configuration management processes.[31]
- *Security Assessments.* This control description referenced an FDIC policy that described the frequency for performing security control assessments. However, the FDIC changed the frequency requirements in August 2012 without updating the security plan.

In addition, we noted that ten separate control descriptions in the security plan referenced the FDIC's previous change management system, Remedy, rather than ServiceNow, which has been in use since October 2016.

A number of FDIC stakeholders rely on information in security plans to make risk management decisions. For example, independent assessors use the information referenced above to plan and conduct security control assessments. Inaccurate

[31] We reported this weakness in our FISMA audit report issued in 2017. In that report, we recommended that the CIO revise the configuration management plans for the FDIC's general support systems, including the Windows Server operating system. The CIO concurred with our recommendation and completed corrective actions.

security control descriptions could result in erroneous control testing, or untested controls. In addition, the FDIC's authorizing official uses security plan information (together with other information describing the security state of information systems) to authorize systems to operate and to determine whether to accept the associated risk. Inaccurate security control descriptions could negatively affect the integrity of these decisions.

Ineffective Efforts to Update Security Plans

The CCA Program's *CCA Methodology* document, which details the FDIC's security control assessment process, states that security plans should be periodically assessed and updated to ensure they accurately describe the information system's security controls. The FDIC addressed this requirement through two separate activities: (1) security control assessments performed by Blue Canopy and (2) periodic reviews of security plans conducted by ISMs. As described below, these activities did not ensure that the security plan for the Windows Server operating system remained current.

Security Control Assessments. Blue Canopy reviewed selected control descriptions in the security plan as part of its December 2016 security controls assessment. The firm identified eight instances in which control descriptions in the plan did not accurately describe the controls' implementation. Blue Canopy created a POA&M which recommended that the FDIC update all security control implementation details in the security plan for all components of the system. However, the corrective action plan that the FDIC developed and approved for this POA&M only addressed the eight specific discrepancies identified by Blue Canopy and did not require a comprehensive review and update of the security plan. As a result, the FDIC corrected the eight discrepancies and closed the POA&M, without further action to review and update the remaining security control descriptions.

ISM Reviews. The security plan states that DIT's ISM reviews the plan as needed, but not less than annually, to ensure that it addresses system and organizational changes. Such reviews of security plans for completeness and accuracy serve an important purpose. However, we found that they do not promote the completeness and accuracy of security plans as changes to security controls occur. Instead, these reviews help to identify changes requiring plan updates only after they occur. We also found an inherent weakness in the design of the ISM review. ISMs lack a detailed real-time awareness of all currently implemented security controls that is critical for effective security plan review.[32]

[32] Stakeholders working in various components of the CIO organization can make IT network, infrastructure, system, and process-oriented changes that impact security controls and, in turn, the accuracy of security plans. ISMs typically do not have responsibility for designing or implementing these controls and, therefore, may not be aware of changes to the controls.

We notified CIO organization officials in June 2017 about our concerns regarding the accuracy of security control descriptions in the Windows Server operating system security plan. These officials acknowledged that the plan required updating. In November 2017, the Deputy Director for ISB informed us that DIT updated its *Change Management Process* document to include requirements to update security plan control descriptions when needed. However, this change only applied to the configuration-related controls managed by DIT, a small subset of the FDIC's overall security controls, and did not ensure that control descriptions for other types of security controls will be updated in a timely manner.

Recommendations

We recommend that the CIO:

7. Update the security plan for the Windows Server operating system to reflect current security controls.

8. Define roles and responsibilities to ensure FDIC personnel update security plans as security controls change.

FDIC Comments and OIG Evaluation

The CIO Organization provided a written response, dated October 31, 2018, to a draft of this report. The response is presented in its entirety in Appendix 5. The CIO Organization concurred with all eight of the report's recommendations. The CIO Organization completed actions to address two of the recommendations and plans to complete actions to address the remaining six recommendations by November 29, 2019. These remaining six recommendations will remain open until we confirm that corrective actions have been completed and are responsive. Appendix 6 contains a summary of the FDIC's corrective actions.

We also provided Blue Canopy with a draft copy of our report for its review. We considered Blue Canopy's informal feedback and made certain changes that we deemed appropriate in finalizing the report.

Objective

The objective of the audit was to determine whether the FDIC established and implemented controls for managing changes to its Windows Server operating system that were consistent with Federal requirements and guidelines.

We conducted this performance audit from March 2017 through August 2018 in accordance with generally accepted government auditing standards. Those 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

To address the audit objective, we:

- Reviewed the FDIC's policies, procedures, and guidelines for managing changes to the baseline configuration for the Windows Server operating system and applying patches to the system, including:
  - *Change Management Process* document, Version 1.3, (August 1, 2014);
  - *CCA Methodology*, Version 2.1, (February 2017);
  - Policy 16-005, *Policy on Secure Baseline Configuration Guides*, (December 9, 2016); and
  - Policy 15-003, *Policy on Security Patch Management*, (October 2, 2015).
- Analyzed relevant security control documentation, such as the baseline configuration, security plan, and vulnerability assessment results for the Windows Server operating system;
- Examined CCA Reports prepared by Blue Canopy in 2016 and 2017 for selected information systems and common controls;
- Spoke with FDIC personnel who had configuration management responsibilities, including the DIT ISM, Blue Canopy personnel, and staff in DIT ISB and the Office of the CISO; and

- Reviewed change management records in ServiceNow and configuration management information in IBM's BigFix tool and Tenable SecurityCenter. The FDIC used BigFix to install security patches and SecurityCenter to track, manage, and report vulnerabilities identified through its scanning processes.

As part of our work, we selected a sample of security patches and configuration changes for detailed review. Specifically, we judgmentally selected:

- 20 of 286 security patches issued by the Microsoft Corporation during 2016 for the Windows Server 2008 and 2012 operating systems; and
- 10 of 53 configuration changes to the baseline configuration for the Windows Server operating system implemented by CIO Organization stakeholders in 2016.

We confirmed that the FDIC applied all 20 patches and updated its baseline configuration to reflect the 10 changes. However, we could not assess the FDIC's handling of these changes (including whether the FDIC properly approved and timely implemented them) because the FDIC lacked current policies and procedures against which we could assess compliance. In addition, DIT personnel did not consistently record in ServiceNow information necessary for us to assess change management activities. Further, DIT did not maintain readily available historical records necessary to allow us to measure the timeliness of its patching activities.

As described in our report, we identified concerns regarding the depth and coverage of security control assessments for the Windows Server operating system. Based on these concerns, we expanded our audit procedures to include five CCA Reports covering the Data Communications system, Midrange Servers system, and certain common control activities.[33] Blue Canopy completed these CCA Reports in 2016 and 2017. We judgmentally selected these systems and common control activities based on their security classification and broad impact on information security at the FDIC.

We evaluated the establishment of controls for consistency with relevant portions of the following Federal requirements and guidelines.

- The Government Accountability Office *Standards for Internal Control in the Federal Government*; and

[33] The Data Communications system and Midrange Servers system are 2 of 13 general support systems maintained by the FDIC. The Data Communications system consists of the FDIC's communications infrastructure that provides computing device connectivity among all FDIC offices. The Midrange Servers system provides hosting platforms for FDIC applications and software. Common controls are security controls inherited by one or more organizational information systems. Weaknesses related to common controls, therefore, have a broader impact than controls that provide security for only one information system.

- NIST security standards and guidelines, including:
  - FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
  - SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*;
  - SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
  - SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*;
  - SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
  - SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*;
  - SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*; and
  - NIST's *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management*.

The scope of this audit excluded an assessment of configuration management controls related to IT programs or applications that run on the Windows Server operating system.

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.

Term	Definition
Authorizing Official	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation. [OMB Circular No. A-130]
Baseline Configuration	A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. [NIST SP 800-128]
Category of Change	The *Change Management Process* document defines three categories of changes: pre-approved, emergency, and normal. Pre-approved changes are routine changes that are easy to implement and present little or no risk to system operation. These changes do not require Change Control Board approval. Normal changes are all other changes that are not emergency or pre-approved. Normal changes require Change Control Board approval before implementation. Emergency changes are changes that must take place on an accelerated timeline to resolve a current or impending stoppage of critical business function(s), production-down issue(s), or significant degradation in IT services. [Based on DIT's *Change Management Process* document]
Common Control	A security control that is inherited by one or more organizational information systems. [NIST SP 800-37, Revision 1]
Computer Security Incident Response Team	The FDIC's Computer Security Incident Response Team investigates and tracks all reported information security incidents, and reports those incidents to the CISO and other officials responsible for the security of the FDIC resource or information. [FDIC Circular 1360.12, *Reporting Information Security Incidents*]
Configuration Management	Configuration management is the collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. [NIST SP 800-128]
Configuration Management Plan	A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. [NIST SP 800-128]
Credentialed Scan	NIST SP 800-53, Revision 4, recommends that organizations use privileged access when conducting vulnerability scans of IT systems and devices. The use of privileged access allows the scanning tool to log into the device being scanned so the tool can conduct a thorough inspection of the device for vulnerabilities. Such scans are sometimes referred to as "credentialed" scans because of their use of privileged (or administrative) access credentials to log into the system. [Based on NIST SP 800-53, Revision 4, with OIG clarification]
Flaw Remediation	Flaw remediation involves identifying, reporting, and correcting information system flaws, such as unapproved configuration settings and missing patches. [Based on NIST SP 800-53, Revision 4]
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. [NIST SP 800-18, Revision 1]

Term	Definition
Information Security Manager (ISM)	ISMs serve within FDIC divisions and offices by providing a business focus on information security. ISMs coordinate with the CIO Organization to ensure the establishment of appropriate security controls to protect their respective division or office's information and information systems. ISM responsibilities include educating employees and contractors on how to properly safeguard FDIC information; assessing system security levels; ensuring that new and enhanced systems address security requirements; and promoting compliance with security policies and procedures. [Based on information from the CIO Organization Web site, with OIG clarification]
Internal Control	A process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. [Government Accountability Office's *Standards for Internal Control in the Federal Government*]
Organizational Conflict of Interest	An organizational conflict of interest may exist when a party to an agreement has a past, present, or future interest related to the work performed (or to be performed), which may diminish its capacity to provide impartial, technically sound, objective service or results in an unfair competitive advantage. [NIST SP 800-35, *Guide to Information Technology Security Services* (October 2003)]
Personally Identifiable Information	Personally identifiable information is any information about an individual which can be used to distinguish or trace that individual's identity, or any other personal information which is linked or linkable to that individual. Personally identifiable information includes, but is not limited to, the personal data of customers of financial institutions (collected by FDIC via receivership/or examination activities) as well as employees, contractors, and visitors to the FDIC. [FDIC Privacy Program Web site]
Plan of Action and Milestones (POA&M)	An internal management tool used by agency CIOs, information security personnel, program officials, and others to track the progress of corrective actions pertaining to information security vulnerabilities. POA&Ms assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions pertaining to security vulnerabilities found in programs and information systems. [Based on NIST SP 800-37, Revision 1, with OIG clarification]
Questioned Costs	Costs questioned by the auditor because of an audit finding: (1) which resulted from a violation or possible violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the use of Federal funds, including funds used to match Federal funds; (2) where the costs, at the time of the audit, are not supported by adequate documentation; or (3) where the costs incurred appear unreasonable and do not reflect the actions a prudent person would take in the circumstances. [Circular No. A-133, *Audits of States, Local Governments, and Non-Profit Organizations*] Costs that are questioned by the OIG because of an alleged violation of a provision of a contract. [5 U.S.C. app. § 5(f)(1)(A)]

Term	Definition
Rework	Rework means services required to correct errors and/or deficiencies that are the result of inadequate, substandard or less than the highest standards of performance by vendor personnel (including arising from inadequate training or preparation of Vendor personnel and/or failure to abide by standard operating procedures). According to the FDIC's contract with Blue Canopy, the "Vendor shall complete Rework at no charge to FDIC unless and then only to the extent the Rework is caused by events outside of Vendor's reasonable control and based upon: (i) FDIC providing incorrect requirements/specifications to Vendor personnel; or (ii) express instruction to Vendor personnel by FDIC. Vendor shall in all cases make Commercially Reasonable Efforts to promptly bring to FDIC's attention any requirements, specifications or instructions which Vendor becomes aware are incorrect and likely to result in Rework." [Contract number CORHQ-14-C-0769]
Security Assessments	Security assessments involve assessing the security controls in the information system and its environment of operation at an organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. [NIST SP 800-53, Revision 4]
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation. [OMB Circular No. A-130] NIST requires agencies to assign a security category of low, moderate, or high to their information and information systems. The security category influences the selection of security controls. [See NIST FIPS Publication 199]
Security Controls	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [OMB Circular No. A-130].
Security Operations Center	A centralized team of information security professionals that investigates and addresses computer security vulnerabilities and incidents. [Based on FDIC Breach Response Plan, Version 2.4]
Security Plan	A formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-37, Revision 1]
System Development Life Cycle	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal. [NIST SP 800-137]
Systemically Important Financial Institutions	Financial institutions whose distress or disorderly failure, because of their size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity. [Financial Stability Board]
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [NIST SP 800-128]

Appendix 3 Acronyms and Abbreviations

Blue Canopy	Blue Canopy LLP
CAC	Corrective Action Closure
CCA	Continuous Controls Assessment
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DIT	Division of Information Technology
DOA	Division of Administration
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
FISMA 2014	Federal Information Security Modernization Act of 2014
ISB	Infrastructure Services Branch
ISM	Information Security Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
P.L.	Public Law
POA&M	Plan of Action and Milestones
SP	Special Publication

Appendix 4 Untested Security Controls

In addition to the concerns noted in the *Inadequate Depth and Coverage of Assessments* section of our report, the table below identifies additional control activities that we concluded were not subject to implementation testing when appropriate.

	Control Activity Recommended by NIST SP 800-53
	Data Communications General Support System ***December 2016 and August 2017 CCA Reports***
1.	Allocate audit record (i.e. system log) storage capacity in accordance with organization-defined audit record storage requirements.
2.	Retain audit records for an organization-defined time period to provide support for after-the-fact investigations of security incidents.
3.	Document configuration change decisions associated with the information system.
4.	Implement approved configuration-controlled changes to the information system.
5.	Include appropriate information system security strength requirements in acquisition contracts.
	Midrange Servers General Support System ***October 2016 CCA Report***
6.	Document and monitor individual information system security training activities.
7.	Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
8.	Test the contingency plan for the information system at an organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.
9.	Update the system security plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
	Common Controls ***January 2016 and December 2016 CCA Reports***
10.	Conduct backups of system-level information contained in the information system at organization-defined frequencies that are consistent with recovery time and recovery point objectives.
11.	Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
12.	Coordinate incident handling activities with contingency planning activities.
13.	Scan for vulnerabilities in information systems in accordance with organization-defined requirements.
14.	Remediate legitimate vulnerabilities within organization-defined timeframes in accordance with an organizational assessment of risk.
15.	Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides.
16.	Screen individuals prior to authorizing access to the information system.
17.	Rescreen individuals according to organization-defined frequencies.
18.	Upon termination of individual employment, retain access to organizational information and information systems formerly controlled by terminated individual.

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Office of the Chief Information Officer

DATE: October 31, 2018

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

THROUGH: Howard G. Whyte **/Signed/**
Chief Information Officer and Chief Privacy Officer

FROM: Zachary N. Brown **/Signed/**
Chief Information Security Officer

Russell G. Pittman **/Signed/**
Director, Division of Information Technology

SUBJECT: **Management Response to the Draft Audit Report Entitled *Security Configuration Management of the Windows Server Operating System* (Assignment No. 2017-009)**

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the FDIC's *Security Configuration Management of the Windows Server Operating System* issued October 9, 2018. We value the independent insights and opinions of the audit team and the perspective they provided.

We appreciate the OIG's evaluation, and we expect that the actions taken in response to this draft report will further enhance the FDIC's configuration management controls, improve change management decisions, and reduce risk to the Corporation. As the report indicates, the Corporation has implemented a comprehensive set of activities to strengthen policy and procedures for managing the configuration of FDIC systems. During the course of the audit (March 2017 – September 2018), the CIO Organization (CIOO) issued a Change Management Policy, Change Management Procedure, and a new work instruction to explain the use of FDIC's automated change management system. The new policy, procedure, and work instruction will help ensure appropriate implementation of FDIC's change management process, including for the Windows Server operating system.

In its report, the OIG audit team made eight (8) recommendations to the CIOO. We have carefully considered and concur with each of the recommendations. The CIOO has already completed actions for two (2) of the eight (8) recommendations. This response outlines the CIOO's completed or planned corrective actions and the corresponding completion dates.

We look forward to continuing our productive dialogue in the coming months on the FDIC's efforts to address the areas noted in the report.

MANAGEMENT RESPONSE

Recommendation 1

We recommend that the CIO:

1. Train personnel on their updated roles and responsibilities as defined in the revised configuration management policies and procedures.

   Management Decision: Concur

   Corrective Action:

   At the time of this audit's field work, one round of training (six training sessions) on the new Change Management process had taken place (September 2017). By the end of October 2017, a new Change Management Process and Procedure had been released, but the accompanying work instruction and policy had not yet been released.

   A Work Instruction on how to use ServiceNow to implement the Change Management process was released in June 2018. The Change Management Policy was released in mid-July 2018. Ten training sessions on the new process, following the technical guidance in the Change Management Work Instruction, took place between June 25th through July 19th 2018. In addition, the training was recorded and posted to the ISB Change Management SharePoint site on July 25, 2018, along with the Change Management process documentation (Policy, Process, Procedure, Work Instruction and the CCB and CAB/CTRB Charters).

   Estimated Completion Date: Completed – July 2018.

Recommendation 2

We recommend that the CIO:

2. Establish and implement controls to ensure that CIO Organization policies and procedures are established before deploying new or modified IT processes or programs.

   Management Decision: Concur

   Corrective Action:

   CIOO will establish and implement procedures within existing governance frameworks to ensure appropriate policies and procedures are in place prior to deployment or modification of IT processes, projects, and programs.

Estimated Completion Date: November 29, 2019

Recommendations 3

We recommend that the CIO:

3. Establish requirements to ensure the independence of security control assessors.

Management Decision: Concur

Corrective Action:

OCISO will review current FDIC policies, procedures, or guidance associated with security controls assessments and will establish requirements to ensure adequate independence of security control assessors.

Estimated Completion Date: June 30, 2019

Recommendation 4

We recommend that the CIO:

4. Establish and implement procedures to ensure that contractor-submitted CCA Reports are reviewed for consistency with applicable requirements in contractual agreements and that such reviews are documented.

Management Decision: Concur

Corrective Action:

OCISO will develop and implement a CCA report review procedure to show that contractor-submitted CCA reports are appropriately reviewed for consistency with applicable requirements as detailed in contractual agreements.

Estimated Completion Date: June 30, 2019

Recommendation 5

We recommend that the CIO:

5. Require that CIO Organization management ensure the sufficiency of CCA Report reviews and provide feedback when review activities are deemed insufficient.

Management Decision: Concur

Corrective Action:

OCISO will establish and implement a CCA report review procedure to ensure CCA reports are reviewed for sufficiency by CIO organization management and feedback is communicated when review activities are deemed insufficient.

Estimated Completion Date: June 30, 2019

Recommendation 6

We recommend that the CIO:

6. Recover $1,080 in questioned costs paid to Blue Canopy.

Management Decision: Concur

Corrective Action:

CIOO has recovered the $1,080 paid to Blue Canopy. NFE shows that Blue Canopy credit invoice # 705211 for ($1,080) was approved on March 6, 2018.

Estimated Completion Date: Completed – March 2018.

Recommendation 7

We recommend that the CIO:

7. Update the security plan for the Windows Server operating system to reflect current security controls.

Management Decision: Concur

Corrective Action:

The WinServ GSS system owner will review and update the security plan for the Windows Server operating system to reflect the current security controls requirements.

Estimated Completion Date: May 30, 2019

Recommendation 8

We recommend that the CIO:

8. Define roles and responsibilities to ensure FDIC personnel update security plans as security controls change.

   Management Decision: Concur

   Corrective Action:

   The CIOO will ensure that the roles and responsibilities for review of, and changes to security plans are delineated, documented, and shared with all appropriate FDIC personnel.

   Estimated Completion Date: March 20, 2019

If you have any questions regarding this response, please contact Kim Farrell, Acting Chief, Audit and Internal Control Section, DIT on 703-516-5101.

cc: E. Marshall Gentry, Deputy Director, DOF, Risk Management and Internal Controls
Greg Kempic, DOF, Risk Management and Internal Controls
Mittal Desai, Deputy Chief Information Security Officer
Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Farhan H. Khan, Acting Deputy Director, DIT, Business Administration Branch

Appendix 6 | Summary of the FDIC's Corrective Actions

This table presents management's responses 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	Actual or Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC trained personnel on their updated roles and responsibilities as defined in revised configuration management policies and procedures during September 2017 (six sessions) and June/July 2018 (ten sessions). The second set of training sessions addressed a new Work Instruction on how to use ServiceNow to implement the CIO Organization's change management process.	July 19, 2018	$0	Yes	Closed
2	The FDIC will establish and implement procedures within existing governance frameworks to ensure appropriate policies and procedures are in place prior to deploying or modifying of IT processes, projects, and programs.	November 29, 2019	$0	Yes	Open
3	The FDIC will review its policies, procedures, or guidance associated with security controls assessments and establish requirements to ensure adequate independence of security control assessors.	June 30, 2019	$0	Yes	Open
4	The FDIC will develop and implement a review procedure to show that contractor-submitted CCA reports are appropriately reviewed for consistency with applicable requirements in contractual agreements.	June 30, 2019	$0	Yes	Open
5	The FDIC will establish and implement a review procedure to ensure CCA reports are reviewed for sufficiency by CIO Organization management and feedback is communicated when review activities are deemed insufficient.	June 30, 2019	$0	Yes	Open
6	The FDIC recovered the $1,080 in questioned costs paid to Blue Canopy.	March 6, 2018	$1,080	Yes	Closed
7	The FDIC will review and update the security plan for the Windows Server operating system to reflect current security controls requirements.	May 30, 2019	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Actual or Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
8	The FDIC will ensure that roles and responsibilities associated with reviewing and updating security plans are delineated, documented, and shared with all appropriate FDIC personnel.	March 20, 2019	$0	Yes	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.