Office of Inspector General

Office of Program Audits and Evaluations
Report No. EVAL-17-005

The FDIC's Controls over the Information Technology Hardware Asset Management Program

June 2017

Office of Inspector General

Executive Summary

The FDIC's Controls over the Information Technology Hardware Asset Management Program

Report No. EVAL-17-005
June 2017

Why We Did The Evaluation

The FDIC uses information technology (IT) hardware assets, among other things, for personal computing throughout the Corporation, supporting network operations, and providing communications connectivity. At the time of our fieldwork, the FDIC had 38,796 IT hardware items in inventory, adjusted for depreciation, with a reported value of approximately $34.8 million. Those items include laptops, workstations, desktops, tablets, printers, scanners, servers, drives, routers, mainframes, and other equipment. With a program of this size, affecting every FDIC division and office, IT hardware assets are vulnerable to several risks, including inefficient or costly procurement, delays in deployment, equipment theft and obsolescence, and data loss. The FDIC's mobile workforce of examiners and distributed field office structure heightens the need for strong controls.

Asset Management Life Cycle Program Objectives

- To promptly procure and deploy required equipment for business operations.
- To keep track of the location of equipment to help prevent loss and theft.
- To maximize the utility of equipment by adhering to replacement schedules and disposing of equipment in a timely manner.
- To ensure sensitive data are erased or removed from equipment prior to repair, return to inventory, or disposal.

The FDIC's Division of Information Technology (DIT) is responsible for managing the Corporation's IT hardware assets, from procurement through disposal, which is referred to as the asset management life cycle (AMLC) in corporate policy. DIT works with the Division of Administration and a contractor to manage the program using an Enterprise Asset Management System (EAMS).

The objective of this evaluation was to evaluate to what extent the FDIC has established key controls to mitigate risks associated with the FDIC's IT hardware asset management program. To conduct our review, we identified program objectives that corresponded to the AMLC, identified potential risks to achieving those objectives, and identified and evaluated program controls to address or mitigate those risks.

Evaluation Results

The FDIC had established some key controls over the IT hardware asset management program, including policies and procedures that specified roles and responsibilities for employees and contractors. However, we found that the FDIC needs to update its policies and procedures and strengthen its controls in most aspects of the program. Further, data needed to manage the program was frequently unreliable. Collectively, these weaknesses create an environment in which the FDIC is vulnerable to ineffectively managing IT hardware assets or having them lost or stolen.

Strengthening Controls Related to Procuring and Deploying Assets. The FDIC had developed several reports to track IT asset procurements and deployment, but there are no procedures as to how the reports should be used. In addition, EAMS reports were not always accurate. For example, one report inaccurately showed that 74 percent of procurement orders had not been received for over 6 months, with some of the procurement orders dating back years. DIT personnel provided supplemental spreadsheets that were used to reconcile and more accurately track the procurement orders. Further, several key data fields in EAMS were often blank or unreliable. For example, 64 percent of the IT assets listed in the system were incorrectly valued at $0. As a result, the FDIC was unable to accurately value its IT assets or evaluate the timeliness of receiving assets and providing them to users.

Enhancing Controls for Tracking and Protecting IT Assets. The FDIC had not effectively implemented controls in this area. Physical inventory results showed few missing assets; however, procedures for conducting such an inventory do not reflect current practices. Further, EAMS showed that 40 of the 178 employees (22 percent) who separated from the Corporation between November 2015 and February 2016 still had at least one IT asset assigned to them in the system. In addition, we identified 16 individuals who had a combination of system access permissions that created weaknesses in the segregation of duties. Moreover, DIT's contractor had not uploaded equipment hand receipts, forms used to assign asset custody, into the system for 15 of 36 laptops that we tested and hand receipt dates were missing for 33 percent of deployed laptops and 46 percent of deployed desktops. Overall, such control weaknesses increase the risk that individuals could misuse or steal IT assets and not be detected.

Using EAMS Data to Monitor and Inform Technology Refresh Decisions. DIT established a Technology Refresh Schedule that is intended to guide IT asset procurements for the next 7 years. DIT management considers IT asset useful life, breakage, and financial assessments in making replacement decisions. However, DIT needed to establish procedures for using the schedule, together with EAMS, to make informed decisions about an asset's useful life. We found that a number of deployed assets were more than 2 years beyond their useful life when compared to the refresh schedule and some assets remained in an end-of-life status for an extended period of time. DIT officials noted these results may reflect situations where it made operational sense to exceed the technology refresh guidelines.

Verifying that Data are Properly Protected Before Disposal or Repair. The FDIC had procedures in place for inventorying and securing hard drives once they had been removed from an IT asset prior to disposal or repair. However, DIT staff or its contractors did not always record in EAMS whether or not the drives had been encrypted to achieve adequate data security.

Addressing Data Reliability and Reporting Issues in the New EAMS. In October 2016, DIT implemented a new EAMS as the FDIC's IT asset management tracking system of record. DIT officials told us the new EAMS would address many of the reporting issues experienced under the prior EAMS. Notably, as of the end of our evaluation, DIT had delayed correcting EAMS data. Until DIT corrects EAMS data, key information will not be reliable and will hinder meeting program objectives.

Recommendations and Corporation Comments

We made nine recommendations for the FDIC to enhance AMLC policies and procedures to reflect current practices; strengthen AMLC controls to better ensure program objectives are met; and improve EAMS data entry, reliability, and reporting to support IT asset management and decision-making. The FDIC concurred with our recommendations and proposed actions responsive to the recommendations to be completed by October 2017.

Contents

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

Office of Program Audits and Evaluations
Office of Inspector General

DATE: June 8, 2017

MEMORANDUM TO: Lawrence Gross, Jr.
Chief Information and Privacy Officer

Russell G. Pittman, Director
Division of Information Technology

/Signed/
FROM: E. Marshall Gentry
Assistant Inspector General for Program Audits and Evaluations

SUBJECT: *Controls over the Information Technology Hardware Asset Management Program* (Report No. EVAL-17-005)

This report presents the results of our evaluation of the Federal Deposit Insurance Corporation's (the FDIC or the Corporation) controls over the information technology[1] (IT) hardware asset management program. According to the Division of Information and Technology's (DIT) IT enterprise asset management system (EAMS), as of August 3, 2016, the FDIC had 38,796 IT hardware items in inventory valued at approximately $34.8 million. Those IT hardware items include laptops, workstations, desktops, routers, Personal Digital Assistants (PDA), tablets, printers, scanners, servers, drives, mainframes, and other equipment. The FDIC uses these IT hardware assets for, among other things, personal computing throughout the Corporation, supporting network operations, and providing communications connectivity.

With a program of this size, affecting every FDIC division and office, IT hardware assets are vulnerable to several risks, including inefficient or costly procurement, delays in deployment, equipment theft and obsolescence, and data loss. The FDIC's mobile workforce of examiners and distributed field office structure heightens the need for strong controls.

Our objective was to evaluate to what extent the FDIC has established key controls to mitigate risks associated with the FDIC's IT hardware asset management program.

To address our objective, we:

- Identified and obtained consensus from DIT regarding the FDIC's IT hardware asset management program objectives.
- Identified potential program risks to achieving the IT hardware asset management program objectives and mapped those risks to the FDIC's existing key controls that would potentially mitigate those risks.

[1] Certain terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Terms*.

- Performed testing in Arlington, Virginia, or relied upon DIT internal reviews and inventories conducted nation-wide, to determine whether key controls adequately mitigated the potential program risk(s).
- Reviewed and analyzed select EAMS data to determine the extent to which data were reliable and used by the FDIC to manage the program.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Appendix 1 of this report includes additional details on our objective, scope, and methodology. Appendix 2 contains a glossary of key terms, and Appendix 3 contains a list of acronyms.

Background

The FDIC's DIT has overall responsibility for the FDIC's IT hardware asset inventory program. This responsibility includes procuring, receiving, deploying, tracking, repairing, replacing, and disposing of IT hardware assets. These responsibilities are described in FDIC Circular 1380.2, *FDIC IT Asset Management Life Cycle Program*. The Circular describes the asset management life cycle (AMLC) as the continuous sequence of processes and changes that occur from the identification of an equipment need through retirement and disposal of the asset.

The table below describes the number of FDIC IT hardware assets, by asset type, and depreciated value as reported in EAMS as of August 3, 2016.[2]

Table: IT Hardware Assets

Equipment Type	Number of Items	Depreciated Value
Workstations – Desktops, PDAs, and Tablets	9,441	$219,681
Laptops	8,931	$9,046,843
Printers	3,034	$772,980
Servers, Processors, and Storage Equipment	2,057	$5,618,955
Scanners	1,406	$123,675
Drives	530	$4,240,941
Mainframes	3	$1,299
Service Support Contracts*	4,077	$4,057,599
Network Devices – Firewalls, Routers, and Switches	3,340	$3,870,512
Other Equipment**	5,977	$6,834,288
Total	**38,796**	**$34,786,773**

Source: *IT Depreciation Report* generated from the EAMS.
*A service contract is a business agreement between a contractor and customer covering the maintenance and servicing of equipment over a specified period. Such a contract is considered an asset with dollar value.
**Other equipment consists of items such as audio/visual, docking stations, keyboards, and monitors.

[2] As discussed throughout this report, we have concerns about the validity and reliability of IT hardware asset data within the EAMS.

Roles and Responsibilities

DIT's Infrastructure Management Section (IMS) provides procurement and oversight management of IT hardware assets. IMS's mission is to ensure that IT asset procurement, asset management, and infrastructure contracting programs are effective.

- *IT Asset Procurement*: IMS gathers IT hardware asset requirements from FDIC divisions and offices and works with the FDIC's Infrastructure Services Contractor (Contractor) or the FDIC's Division of Administration (DOA) to procure IT hardware assets. The procurements are made in accordance with the FDIC procurement policies contained in the *FDIC Acquisition Procedures, Guidance, and Information* documentation.

- *Asset Management*: IMS has day-to-day responsibility for overseeing the FDIC's IT hardware asset management program. Once the FDIC procures the IT hardware asset, IMS tracks the asset, from receipt through disposal, in EAMS. This includes tracking the asset through deployment to users, conducting inventories, coordinating asset repairs, and overseeing asset disposal.

- *Infrastructure Services Contractor*: The Contractor, along with federal staff, implements many of the daily activities related to managing IT hardware assets and performs a number of AMLC activities, including procuring and receiving assets, issuing hand receipts to establish asset custody, performing asset inventories, and entering information into EAMS. Various DIT branches provide technical monitors and subject-matter experts to inspect work, monitor the contract, and ensure that the Contractor meets all of its terms and conditions.

Evaluation Results

The FDIC had established some key controls for each program objective associated with the IT hardware asset management program, including policies and procedures that specified roles and responsibilities for employees and contractors. These are described in Appendix 4 of our report. However, we found that the FDIC needs to update the following policies and procedures in order to meet program objectives:

- FDIC Circular 1380.1, *Assignment of FDIC Information Technology Hardware Assets*, dated November 10, 2009.
- FDIC Circular 1380.2, *FDIC Asset Management Life Cycle Program*, dated December 7, 2009.
- DIT Policy 05-006, *Policy on IT Asset Management Life Cycle*, dated May 25, 2005.

We also describe in the following sections how weaknesses in controls and data reliability increase risk in the FDIC's IT hardware asset management program.

Strengthening Controls for Procuring and Deploying IT Assets

Procurement

In September 2015, DIT developed a Technology Refresh Schedule (TRS)[3] that tracks the age, useful life, and need for equipment replacement. The TRS also compares budget figures to actual expenditures. The TRS is a useful tool for projecting future business equipment needs for the Corporation. However, throughout the course of our review, the FDIC had not established procedures as to (i) how the TRS would be developed and used in the IT asset procurement process; nor (ii) how purchases made outside of the TRS could be justified, documented, and approved.

DIT also developed an *On Order Report* to track equipment it had ordered from a vendor but that it did not receive. DIT coordinated with DOA on a weekly basis to track the progress of IT assets appearing on the *On Order Report.* Again, we noted that the FDIC had not developed procedures for how the report was to be used in the procurement process. We analyzed the *On Order Report* dated February 25, 2016, and noted that equipment was on the report for a significant period of time. Almost 74 percent of the open orders had been on order for more than 6 months, with some of the orders dating back to 2007.[4] Absent procedures establishing expectations and accountability for the report, it will have limited positive impact on intended control improvements over procurements.

In addition, we analyzed information regarding the purchase prices of IT assets from DIT in conjunction with the *IT Depreciation Report* dated March 3, 2016. The *IT Depreciation Report* contained EAMS data for an IT asset's unit price, presented the length of time the asset had been held in inventory, and calculated the depreciated value (reduced value due to age) of each IT asset over a standard 5-year useful life. Our analysis of the report observed:

- About 64 percent of the 38,730 IT assets listed had an inaccurate unit price of $0.
- Two items had negative unit prices that together, totaled nearly $300,000.
- Six line items totaling almost $13 million appeared to be for bulk purchases that were not assigned to individual assets.
- Duplicate entries totaling about $1.5 million related to these bulk totals, where the bulk line item existed but separate asset unit prices were also recorded.

We noted that DIT did not consider unit price to be one of the critical data elements that must be reviewed for accuracy. Correct asset valuation is important for asset management decision-making. Further, if the unit price is incorrectly recorded in EAMS, the depreciated values of IT

[3] The TRS is established every year, then periodically reviewed and updated based on priority changes. The useful life of the assets is determined using industry best practices, subject-matter expert experiences, and, in some cases, is discussed with independent research and advisory groups that provide IT-related insight. Generally, the number of pieces of equipment identified for replacement varies from year to year, depending on the composition of the refresh projects.

[4] DIT personnel stated that some of the old items were the result of problems with a prior asset management system, which would not allow cancellation of individual line items when a change occurred, such as to the amount ordered.

assets cannot be properly computed and recorded, and internal FDIC reports of depreciated values could be materially misstated. DIT officials informed us that the FDIC uses the depreciated value data in the *IT Depreciation Report* to determine the value of the FDIC's IT hardware assets for insurance coverage purposes. Therefore, it is important that the unit price field be correct so that the FDIC's calculation of depreciation is accurate and the FDIC is paying appropriate insurance premiums.

Receipt

We attempted to analyze the cycle time between when an IT asset was procured and received by the FDIC. However, EAMS could not link procurement and asset information, and DIT could not provide a report that contained both an asset procured and asset received date. Further, when we analyzed the reliability of the received dates contained on a separate EAMS *Asset Disposal* report, we determined that over the course of 5 years (from January 2011 through December 2015), the report lacked a date for when the IT asset was received for almost 18 percent of the assets. DIT identified the received date as one of the critical data elements that must be monitored for accuracy.

We noted that a subsequent report from May 11, 2016, showed only 1.5 percent of the IT assets were missing the received date. However, due to the number of missing dates for receipt of IT assets from the earlier years, we were unable to complete our analysis of asset procurement to asset receipt timeframes. This lack of complete and accurate information makes it difficult for DIT to manage the program and gauge procurement efficiency.

Deployment

We identified another control practice that the FDIC had implemented, but not reflected in procedures, to help ensure that IT assets were deployed in a timely manner. Specifically, FDIC developed a *New Equipment* report that shows an aging of higher-dollar-value assets in inventory. The *New Equipment* report dated December 2015 listed nearly $5.7 million in IT assets in inventory, some of which had been in inventory for more than 2 years.[5] For example, in November 2014, DIT purchased two servers valued at $430,000 that were still in inventory almost 2 years later, which typically represents about 40 percent of their useful life. DIT provided a *New Equipment* report dated May 2016 that showed the amount of IT assets in inventory had dropped to $3.4 million.

We also found that approximately 86 percent of 3,400 laptops that were purchased in June 2016 had yet to be deployed as of December 15, 2016. The deployment was delayed to conduct a security assessment. According to the TRS, laptops have a useful life of 3 years, almost 6 months of which had already elapsed prior to deployment. We noted that DIT had significantly reduced the number of laptops in inventory by March 2017 to 30 percent of the 3,400 that had been purchased.

[5] DIT personnel informed us that managers review the *New Equipment* report monthly and that some of the IT assets on the report could have been purchased as part of a project and not used, or may have been purchased as back-up equipment should another piece of equipment fail.

DIT personnel also noted that they rely heavily on the Contractor to deploy IT assets. DIT contractor performance assessments cited concerns related to the timeliness of the Contractor's equipment deployment, which has led to excessive inventory and equipment maintenance contract expirations.[6] In addition, the Contractor had not prepared required *Asset Compliance* and *Asset Activity* reports to measure how timely equipment was deployed.[7] During our evaluation, DIT had placed the Contractor on a performance improvement plan and did not approve performance incentive payments because of the Contractor's unsatisfactory performance.

We attempted to analyze the timeliness of IT hardware asset deployment by requesting that DIT run EAMS-generated reports. However, due to the limitations of EAMS and lack of reporting tools, DIT was unable to provide a report that consistently included the date of an asset's initial deployment.[8] These factors made it difficult to compare the asset receipt date to the initial asset deployment date for a trend analysis and for DIT to monitor deployment trends.

Enhancing Procedures for Tracking and Protecting Assets

IT Asset Inventories

We found that the FDIC was not conducting physical inventories on the schedule outlined in Circular 1380.2. Instead, the FDIC conducted annual inventories of all IT asset types by determining whether the IT asset had been connected to the FDIC network during the past year, a process DIT refers to as verification by exception. If an asset could not be verified by electronic means, DIT would conduct a physical inspection intended to locate the asset. DIT had not formally updated this inventory process change as of January 2017.

We noted that DIT identified only 16 missing portable assets in the annual 2015 inventory, out of the 14,461 tracked portable assets. Further, the 2016 inventory also had a small percentage of missing assets—101 out of the 35,675 active assets that were inventoried at that time. Updating existing procedures to reflect current practices will help ensure that the high rate of accountability is maintained.

We noted that automated inventory practices, such as DIT's verification by exception process, are an acceptable method of identifying the existence of IT assets. However, we did not identify guidance regarding what timeframe would be acceptable in considering an asset to be verified. In our view, DIT's 1-year timeframe for verifying equipment that had been connected to the network could be shortened to help ensure that missing equipment is identified timely.

[6] Maintenance contracts are important to keeping equipment operational and may have expired while the equipment was in inventory without the FDIC receiving any benefit for the cost of the contract.
[7] DIT noted that DIT staff were able to produce other individual reports that collectively included the content listed in the *Asset Compliance* and *Asset Activity* reports.
[8] Reporting problems included the previously mentioned asset received date data quality issues, multiple asset installation dates for a single asset, and asset redeployment dates that overwrote the original date of deployment.

Physical Access Controls and Storage Areas

DIT maintains policies related to physical access controls for the main computer center in Arlington, Virginia, but those policies did not contain requirements for temperature controls. In addition, the FDIC did not have policies in place governing physical access and temperature controls for IT asset storage rooms. DIT Internal Review reports have cited concerns related to temperature controls and physical access to IT asset storage rooms. Our initial observation of storage areas in the FDIC's Virginia Square location identified inadequate cooling in one of the three storage rooms. During a follow-up, we observed that the room was noticeably cooler, with the automatic fan functioning properly. Although DOA is responsible for facilities, including the storage areas for IT asset equipment, DIT should outline requirements for the main computer center and IT asset storage areas to better ensure the assets are protected from damage or misuse.

Separating Employees

According to Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*, dated September 3, 2014, all FDIC-owned property and equipment must be accounted for and returned at the time of separation. The separating employee is responsible for returning all FDIC-owned property and DIT is responsible for certifying that all equipment and related manuals have been returned. Our comparison of EAMS' *Active Assets Report* dated March 8, 2016, to DOA's listing of employees separated from the FDIC, indicated that 40 of the 178 employees (22 percent) who separated from the Corporation between November 20, 2015, and February 23, 2016, still had at least one IT asset assigned to them in EAMS, mostly laptops or PDAs. DIT had not developed a procedure that required a similar comparison to ensure that all IT assets had been returned.[9]

EAMS Access Controls

FDIC Circular 1360.15, *Access Control for Information Technology Resources*, dated February 27, 2009, requires, among other things, that:

- access to IT resources shall be provided for legitimate business use only and only after proper authorization, when required;
- where required, access controls shall be used to enforce the principle of segregation of duties to restrict the level of access and ability provided to any single individual; and
- periodic reviews of access control settings shall be conducted to ensure that appropriate controls remain consistent with existing authorizations and current business needs.

We found that DIT had not established procedures over EAMS access that included guidance for ensuring separation of duties and access monitoring. Specifically, the *Asset Users List* dated February 26, 2016, showed that 16 individuals had a combination of access permissions for both

[9] At the time of our review, we were also conducting a separate evaluation to determine the extent to which the FDIC has established controls to mitigate the risk of unauthorized access to and inappropriate removal and disclosure of sensitive information by separating personnel.

procuring and receiving assets that created segregation of duty control weaknesses. While the list showed the majority of users had a read-only level of access, we found that 16 users had broad access privileges. We found that these personnel likely did not need that broad level of access to complete their duties. Control weaknesses related to segregation of duties and access permissions increase the risk that IT assets could be inappropriately procured or stolen.

IT Asset Custody

A key control in managing IT assets is assigning responsibility and accountability for the asset. FDIC Circular 1380.1 requires that a hand receipt be completed for each IT asset that has been deployed. DIT requires the Contractor to include the asset receipt date in EAMS and upload the hand receipt in the EAMS asset record. Preparing and attaching hand receipts in EAMS provides a record of IT asset custody and accountability. We noted that these requirements were not being adhered to:

- The Contractor and FDIC employees were not consistently uploading hand receipts into EAMS. Of the 36 deployed laptops we reviewed as of March 25, 2016, 15 did not have the signed equipment receipt form uploaded to EAMS.[10] In addition, the 2015 DIT physical portable asset inventory reported that equipment hand receipts documenting change of IT asset custody from one employee to another were missing in several instances.

- The Contractor and FDIC employees also were not consistently recording the asset receipt date into EAMS. Our review noted the *Active Assets Report* dated February 25, 2016, contained a large number of missing hand receipt dates in EAMS, including 33 percent of deployed laptops (1,737), 46 percent of deployed desktops (2,706), 54 percent of deployed PDAs (1,526), and 29 percent of deployed computer tablets (66).

DIT's Contractor performance assessments also identified weaknesses and reported the Contractor did not understand its responsibility for tracking assets and recording asset updates in EAMS. A key contract performance indicator for EAMS accuracy requires 80-percent accuracy for the Contractor to be at an acceptable quality level. DIT procedures require preparation of a weekly missing hand receipt report to identify all assets that do not have a hand receipt attached in the EAMS asset record but have a status change to deployed, transferred, or on loan. DIT had not been running this report, or performing other review activities, to identify these data reliability issues. DIT also clarified that the prior IT asset management system employed specific naming conventions for uploading hand receipt attachments, and that, if not followed precisely, this legacy system would not associate the hand receipt with the correct IT asset.

The *Internal Control Standards* set by the Government Accountability Office (GAO) provide that management should establish activities to monitor the internal control system and evaluate the results. In this regard, DIT had conducted numerous internal reviews of the IT asset program at the FDIC's headquarters offices and four regional offices from 2011 through 2015 that included sampling of inventory items, reviewing storage areas, and conducting limited EAMS data reliability assessments. Importantly, these reviews identified that controls needed to be

[10] DIT was able to locate and provided signed hand receipts for these 15 laptops.

improved over IT asset storage and the reliability of EAMS data for hand receipts. These asset custody weaknesses coupled with the segregation of duties and system access permission weakness mentioned earlier increase potential risks that IT assets could be stolen or misplaced.

Using EAMS Data to Inform Technology Refresh Decisions

Replacement

As discussed earlier, in September 2015, DIT established a TRS, which outlines needed IT asset procurements by year for the next 7 years. The TRS documents the estimated useful life of each asset by type and includes the number of years since the last refresh. We reviewed the *Active Assets Report* dated March 10, 2016, to determine how often IT hardware assets were being replaced. Our analysis found that a number of IT hardware assets were 2 years beyond their estimated useful life designated in the TRS. For example, 30 percent of laptops and 17 percent of PDAs were 2 years beyond their estimated useful life.

According to DIT officials, these results may reflect situations where it made operational sense to exceed the TRS guidelines rather than indicating that obsolete assets were being retained past their useful life. They further noted that the TRS needs to be flexible to allow for management discretion but acknowledged that using EAMS data would help DIT make decisions about technology refresh.

Disposal

During our review of IT asset policies, procedures, and processes, we found that DIT has standard operating procedures for disposal of assets based on asset functionality, warranty repairs exceeding cost of replacement, or management decision to retire the asset based on technology or economics. DIT changes an asset from deployed to end-of-life status when it identifies the asset as not qualifying for any future need and ready for disposal. The *Active Assets Report* dated March 10, 2016, showed 4,039 assets in end-of-life status. About 90 percent of those assets were comprised of laptops.[11] We analyzed a sample of 20 laptops, 20 PDAs, 20 printers, and 20 desktops that were in end-of-life status as of March 10, 2016. Our analysis found that 13 of the 80 sampled assets were still in end-of-life status as of May 4, 2016, and had been in end-of-life status for over 6 months. We concluded that a periodic review of assets in the end-of-life status, and a target timeframe within which assets should be disposed of, could lead to more efficient disposal of equipment that is no longer in use.

Verifying that Data Are Properly Protected Before Disposal or Repair

The FDIC has policies and procedures designed to ensure that sensitive data are removed from equipment prior to repair, return to inventory, or disposal, that are described in Appendix 4. As it relates to disposal, we found that DIT had adequate controls over that process, including inventorying each hard drive, disabling the hard drive, and then having the hard drive shredded

[11] These laptops were in this status because the FDIC was in the process of finishing a laptop refresh project which started in September 2015.

by a professional shredding company. Security cameras were also used throughout the process to ensure that the shredding process was recorded.

With respect to repair, DIT removes hard drives before sending computers for repair. DIT's standard computer design does not require that desktop computer hard drives be encrypted but does require they be encrypted for laptops.[12] We noted that the laptop encryption data field was not always completed in EAMS. Specifically, for nine laptops in repair status, three had blank encryption status fields. To ensure sensitive data are protected, the FDIC would benefit from verifying the laptop encryption status of a hard drive within EAMS prior to equipment repair.

Addressing Data Reliability Issues in the New EAMS

According to the *Internal Control Standards*, any agency should be sure to use quality information that is appropriate, current, complete, accurate, accessible, and provided on a timely basis. Management uses such information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks. In this regard, we had a number of challenges obtaining key information related to the management of the IT asset inventory. For example, we were unable to obtain reports for assessing the timeliness of asset procurements or deployments, and we could not obtain a reliable report for the value of the FDIC's inventory. In addition, we had difficulties determining whether separated employees had IT hardware assets assigned to them.

In October 2016, DIT implemented a new EAMS as the FDIC's IT asset management tracking system of record. DIT officials told us the new EAMS would address many of the reporting issues experienced under the prior EAMS system. For example, DIT officials indicated that:

- The new EAMS includes system controls that require certain fields, including unit price, to be populated in order to add a new equipment item to EAMS. This automated control should help ensure that key asset information fields are populated.

- The new EAMS has greater reporting capability for tracking IT asset procurements, how quickly IT assets are received, and how quickly IT assets are deployed to users.

- They had developed new user roles within the new EAMS to improve segregation of duties.

- The new EAMS automatically generates equipment hand receipts, which should reduce the number of hand receipt errors that we identified.

While these steps improve controls, DIT delayed correcting EAMS data to a later date. Until DIT corrects the data, key information used for managing the program will not be reliable and will hinder decision-making related to the AMLC program objectives.

[12] DIT had controls in place for inventorying and securing desktop hard drives.

Conclusion and Recommendations

While DIT has established some key controls over the IT hardware asset management program, the FDIC needs to improve the program by updating and enhancing policies and procedures, strengthening controls, and significantly improving data quality in its IT hardware asset management system. While the new EAMS may address some of the issues identified in our report, until DIT corrects the data, key information used for managing the program will not be reliable and will hinder decision-making related to the AMLC program objectives. Absent control and data quality enhancements, the FDIC is at greater risk of not spending funds wisely and losing or having equipment stolen.

We recommend that the Director, DIT:

1. Enhance AMLC policies and procedures to reflect current practices for procuring, receiving, deploying, tracking, protecting, replacing, and disposing of IT assets.

2. Develop procedures for using the Technology Refresh Schedule as part of the procurement process and resolving open orders that have not been received for an extended period of time.

3. Evaluate inventory timeframes to ensure they provide timely information about an asset's location.

4. Establish procedures to ensure that separated employees have returned all assets assigned to them in EAMS as part of the pre-exit clearance process.

5. Establish controls in EAMS that ensure adequate segregation of duties among individuals responsible for managing IT assets.

6. Review metrics used for data accuracy and timeliness of removing assets from end-of-life status.

7. Establish a process for conducting data reliability reviews of key data elements within EAMS to ensure accuracy and completeness.

8. Establish means for holding DIT and Contractor staff more accountable for ensuring that EAMS data are accurate and complete.

9. Improve IT asset management reporting to obtain reliable information that is timely and useful in managing the AMLC.

Corporation Comments and OIG Evaluation

The Chief Information and Privacy Officer and Director, DIT, provided a response, dated May 26, 2017, to a draft of this report. The response is presented in its entirety in Appendix 5. The Chief Information and Privacy Officer and Director concurred with the nine recommendations, proposed actions responsive to the recommendations, and targeted completion dates from August 4, 2017, through October 6, 2017. These recommendations will remain open until the planned actions are completed. A summary of the Corporation's corrective actions is presented in Appendix 6.

Objective, Scope, and Methodology

Objective

Evaluate to what extent the FDIC has established key controls to mitigate risks associated with the FDIC's IT hardware asset management program.

We performed this evaluation from November 2015 through July 2016 and obtained updated information for some findings as of January 2017. We conducted our evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Scope and Methodology

The scope of this evaluation included the identification of potential program risks and mitigating controls within each program objective in DIT's hardware asset management program. In conducting our work, we obtained preliminary reports from EAMS as of November 20, 2015. As we began analyzing the report data, we determined that the reports did not accurately capture the requested information. We requested new EAMS reports from DIT in February 2016 in order to conduct our analysis. As described in the report, we continued to have concerns with the reliability of data in the EAMS-generated reports.

To address the evaluation objective, the assignment team, in conjunction with DIT, identified the following IT hardware asset inventory program objectives at the onset of the assignment:

- Program Objective 1: To promptly procure and deploy required equipment for business operations.
- Program Objective 2: To keep track of the location of equipment to help prevent loss and theft.
- Program Objective 3: To maximize the utility of equipment by adhering to replacement schedules and disposing of equipment in a timely manner.
- Program Objective 4: To ensure sensitive data are erased or removed from equipment prior to repair, return to inventory, or disposal.

To address our evaluation objective, we gained an understanding of the FDIC's IT asset management program. We met with officials from DIT's Infrastructure Management Section, Operations Section, and Client Services Section; DOA's Acquisition Services Branch; and the Division of Finance's General Ledger Operations and Control Section to obtain an understanding of the program and processes related to the FDIC's IT hardware asset program and reporting. We also discussed DIT's plans to change EAMS.

We identified and became familiar with key applicable IT hardware asset policies, criteria, and guidelines, including, but not limited to:

- FDIC policies;
- DIT and DOA policies and procedures;
- the infrastructure services contract;
- the Acquisition Policy Manual; and
- GAO *Standards for Internal Control in the Federal Government*, September 2014, GAO-14-704G.

We reviewed OIG Evaluation Report No. 03-032, *Life-Cycle Management of Information Technology Assets*, issued July 18, 2003, and an IG Memorandum Entitled, *Controls Regarding the Receipt and Inventory of Information Technology Equipment* (Assignment No. 2012-035), issued May 4, 2012, for purposes of understanding the FDIC's asset management and inventory system. We also reviewed DIT Internal Review reports involving the review of DIT's IT hardware assets. In some cases, we limited testing because of recent DIT internal review efforts and DIT equipment inventories.

We identified controls within the IT hardware asset program and risks related to each program objective. We determined whether the IT asset hardware controls in place successfully mitigate the risks associated with the agreed-upon program objectives. We also validated the accuracy of the information in EAMS, the IT asset management system of record. The universe of assets for the evaluation included the following commonly identifiable, data-bearing, and IT hardware assets: laptops, workstations, desktops, routers, PDAs, tablets, printers, scanners, servers, drives, mainframes, and other equipment.

We used non-statistical methods to review data in EAMS. Non-statistical samples are judgmental and cannot be projected to the population of IT hardware assets. None of the sampling techniques that we used can be used to project to the intended population by standard statistical methods. Data-related checks included:

- analysis of data within EAMS for incorrect or missing fields and
- trend analyses of selected data in EAMS to determine if DIT had established key controls or metrics for managing the AMLC program.

We performed our work at DIT and DOA offices in Arlington, Virginia, and a vendor hard drive destruction facility in Sterling, Virginia.

Glossary of Terms

Term	Definition
Asset Management Life Cycle	The continuous sequence of processes/changes that occur from the identification of an equipment need through retirement and disposal of the asset.
Encrypted	A method to achieve data security through the translation of data into a secret code.
Hand Receipt	Form used to authorize an individual to have IT hardware in their possession and record the assignment/transfer of an IT hardware asset to an individual or back to DIT.
Information Technology	Any equipment or interconnected system of equipment that is used in the creation, conversion, or duplication of data or information.
IT Hardware	The physical, material parts of a computer or other asset such as a printer, scanner, or server. The term distinguishes these fixed parts of a system from the more changeable software or data components which it executes, stores, or carries. The FDIC tracks hardware if one or more of the following criteria are met: (1) the purchase value is at least $500, (2) the asset has the ability to store data, or (3) the asset requires tracking for reasons such as replacement schedules or accountability.
Portable Asset	An IT asset that is intended to be carried with the employee or contractor as they perform the duties of their assignment. Examples of portable IT hardware include, but are not limited to, laptops, PDAs, and cellular phones.
Technology Refresh Schedule	A schedule developed by DIT that tracks the age of equipment, the useful life of the equipment, and the need for replacement. DIT determines the useful life of equipment through industry best practices, subject-matter expert experiences, and, in some cases, independent research and advisory groups that provide technology-related insight.
Unit Price	The cost of an individual piece of equipment. For a bulk purchase of multiple laptop computers, the unit price would be the price of an individual laptop.
Verification by Exception	Verification by exception is accounting for an asset through approved methods other than physical inventory or verification. Methods of verification by exception include, but may not be limited to, custody transactions, usage logs, and discovery by electronic tools.

Abbreviations and Acronyms

Abbreviations	Explanation
AMLC	Asset Management Life Cycle
CIOO	Chief Information Officer Organization
CSS	Client Services Section
DDC	Division of Information Technology Distribution Center
DIT	Division of Information Technology
DOA	Division of Administration
EAMS	Enterprise Asset Management System
FDIC	Federal Deposit Insurance Corporation
GAO	Government Accountability Office
IMS	Infrastructure Management Section
IR	Internal Review
IT	Information Technology
MOU	Memorandum of Understanding
OIG	Office of Inspector General
PDA	Personal Digital Assistant
SOP	Standard Operating Procedure
TRS	Technology Refresh Schedule
USDA	United States Department of Agriculture
WI	Work Instruction

Policies and Procedures for the AMLC

The following are policies and procedures that we identified by program objective and their status, in relation to practices we found in place during our review.

Procuring, Receiving, and Deploying Equipment

Policy and Procedure	Description	Status
Procurement Phase		
The *FDIC Acquisition Policy Manual* issued August 22, 2008, with pedestrian changes through May 15, 2014	The manual applies to all procurement actions awarded by the DOA Acquisition Services Branch. The manual includes guidance on acquisition planning and competition, general contract requirements, and delegations of authority for approval of procurements.	Current
FDIC Circular 1380.2, *FDIC Information Technology Asset Management Life Cycle Program*, dated December 7, 2009	The policy establishes responsibilities within DIT for procuring IT assets in support of corporate needs and requirements.	Did not reflect current practice
Business Administration Branch IMS Designation of Purchasing Agent Standard Operating Procedures dated June 6, 2016	The procedures describe which purchasing agent and method should be used based on a set of determining factors, including dollar amount and complexity of the procurement action. They also generally provide for a segregation of duties between DIT and DOA for IT asset purchases.	Current
Receipt Phase		
FDIC Circular 1380.2, *FDIC Information Technology Asset Management Life Cycle Program*, dated December 7, 2009	The policy requires all IT assets to be received by the DIT Distribution Center (DDC) unless the DIT Asset Manager approves an exception. The policy also requires all IT assets to have unique FDIC identification tags for tracking purposes.	Did not reflect current practice
FDIC Standard Operating Procedure (SOP) 014 *Asset Management DDC Receiving Procedures* dated June 26, 2015	The procedures describe the steps taken by the DDC in receiving and inspecting IT hardware assets, following up on damaged assets, updating EAMS records, and storing equipment in inventory.	Current
Deployment Phase		
FDIC Circular 1380.1, *Assignment of FDIC Information Technology Hardware Assets*, dated November 10, 2009	The policy requires DIT to establish standard IT hardware assignments and deploy IT hardware assets to the appropriate employee or contractor. It also requires employees and contractors to sign an equipment hand receipt form acknowledging responsibility for the IT hardware asset.	Did not reflect current practice
FDIC_SOP-013 *DIT DDC Equipment Distribution*, dated June 28, 2015	The procedures describe the tracking process of transferring IT equipment from the DDC to the regional or headquarters destination, including approval, ticketing, and equipment receipt completion.	Current

Tracking Equipment

FDIC Circular 1380.1, *Assignment of FDIC Information Technology Hardware Assets*, dated November 10, 2009	The policy establishes guidelines and responsibilities for the FDIC's employees and contractors when assigned IT hardware assets. It requires employees and contractors to sign an equipment hand receipt form acknowledging responsibility for the IT hardware asset. It also requires DIT to maintain the equipment receipt form to monitor the transfer of IT hardware assets.	Did not reflect current practice

Policies and Procedures for the AMLC

Policy and Procedure	Description	Status
FDIC Circular 1380.2, *FDIC Information Technology Asset Management Life Cycle Program*, dated December 7, 2009	The policy states DIT is responsible for ensuring the completion of the annual comprehensive hardware asset inventory, the semi-annual portable asset inventory, and periodic spot check inventories. It states that on a periodic basis (semi-annually for portable hardware assets and annually for all other hardware assets), all IT hardware assets shall be inventoried to ensure accountability and physical verification.	Did not reflect current practice
FDIC Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*, dated September 3, 2014	The policy states that all FDIC equipment must be accounted for and returned at the time of separation. Employees are responsible for returning all FDIC-owned property, including, but not limited to, computers, communication devices, and equipment. DIT is responsible for certifying that all IT hardware equipment has been returned.	Current
FDIC_SOP-012 *Asset Management Asset Tracking* dated March 9, 2015	The procedures state that EAMS is the primary source of tracking and ensuring assets are assigned and accounted for. They also require the Asset Manager to prepare a memorandum to the Chief Information Officer and DIT Director certifying annual inventory completion and the percentage of equipment that was verified.	Current
DIT Policy 14-007, *Policy on Physical Access to FDIC Data Centers*, dated December 22, 2014	The policy limits physical access to the FDIC's Virginia Square and Manassas Data Centers based on job responsibilities and requires DIT to annually recertify physical access for individuals.	Current
Using Replacement Schedules and Disposing of Equipment		
FDIC Circular 3200.1, *Disposition of Corporation-Owned Property*, dated August 25, 2004	The policy states DIT is responsible for determining whether IT resources should be redeployed or turned over to DOA for disposition. It also outlines DOA equipment disposition methods, including sealed bid, public auction, transfer, or donation depending on property value.	Current
FDIC Circular 1380.2, *FDIC Information Technology Asset Management Life Cycle Program*, dated December 7, 2009	The policy states that IT assets no longer needed or supported by the Corporation shall be disposed of in accordance with FDIC Circular 3200.1, *Disposition of Corporation-Owned Property*.	Did not reflect current practice
DIT Policy 05-006, *Policy on IT Asset Management Life Cycle*, dated May 25, 2005	The policy defines responsibility for IT assets from initial request through preparation for retirement. DIT is responsible for determining the usage and life expectancy of IT assets.	Did not reflect current practice
FDIC_SOP-015, *Asset Management DDC Surplus Disposal*, last updated December 2, 2015	The procedures require the Asset Manager to issue authorization to contractor staff to retire, trade-in, or dispose of IT assets; the DDC to prepare equipment for retirement, trade-in, or disposal and update EAMS; and DOA to coordinate the asset disposal. The procedures state DIT should retire, trade in, or dispose of IT assets if the asset is no longer functional, the warranty repairs exceed the cost of replacement, or DIT management decides to retire the asset based on technology or economics.	Current

Policies and Procedures for the AMLC

Policy and Procedure	Description	Status
Memorandum of Understanding (MOU) between the United States Department of Agriculture (USDA) and the FDIC for the period October 1, 2015 through September 30, 2016	The MOU establishes the terms and conditions of the FDIC's agreement with the USDA for excess property disposal services, including IT equipment disposal. The agreement contains provisions for the tracking and sale of equipment transferred from the FDIC to the USDA.	Current

Ensuring Sensitive Data Are Erased or Removed from Equipment

The FDIC Circular 1360.9, *Protecting Sensitive Information*, April 30, 2007, with pedestrian changes through October 27, 2015	The circular establishes the FDIC policy on protecting sensitive information collected and maintained by the Corporation and provides guidance for safeguarding the information, including encryption of sensitive information stored on end-user IT equipment.	Current
DIT's Hard Drive Accountability System User Manual for Version 4.0, as of May 12, 2014	The manual describes the FDIC's program to provide a systematic and verifiable method for tracking and physically disabling computer hard drives across the organization.	Current
DIT Policy Number 11-006, *DIT Policy on Hard Drive Sanitization and Destruction*, July 7, 2011	The policy provides guidance on the appropriate handling of computer hard drives removed from service. It describes DIT's responsibilities for retaining and sanitizing hard drives on laptops and servers.	Current
The FDIC's *Acquisition Procedures, Guidance and Information*, updated through October 2015	The guidance contains contracting requirements related to the protection of sensitive information by contractors.	Current
FDIC_SOP-015, *Asset Management DDC Surplus Disposal*, last updated December 2, 2015	The procedures describe the validation inspections required for designated assets and peripherals prior to final disposition through DOA.	Current
The FDIC Work Instruction WI-016, *Asset Management Destruction of the FDIC Data Bearing Devices*, last updated December 15, 2015	The work instructions cover steps taken by the DDC to destroy data bearing devices, including an inspection to ensure the hard drive has been rendered inoperable. They also describe how the DDC has a verification box to sign that final disposition has occurred through shredding.	Current

Corporation Comments

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500

DATE: May 26, 2017

TO: E. Marshall Gentry
Assistant Inspector General for Audits and Evaluations

FROM: Lawrence Gross, Jr. /**Signed**/
Chief Information and Privacy Officer

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

SUBJECT: Management Response to the Draft Evaluation Report Entitled
Controls over the Information Technology Hardware Asset Management Program
(Assignment No. 2015-030)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report on the FDIC's Controls over the Information Technology Hardware Asset Management Program issued April 19, 2017. In its report, the OIG made nine recommendations to the Chief Information and Privacy Officer (CIO). We agree that additional steps should be taken to further enhance the controls supporting the FDIC's Information Technology (IT) Hardware Asset Management program.

We appreciate your staff's evaluation and we expect that the actions taken in response to this draft report will further enhance the FDIC's IT hardware asset management controls, improve asset management decisions, and reduce risk to the Corporation.

This response outlines CIOO's planned corrective action for the nine recommendations directed to the CIO cited in the OIG's report. We have carefully considered and concurred with the nine recommendations. Our detailed response is organized by recommendation and contains actions already completed, planned, or in process.

Corporation Comments

MANAGEMENT RESPONSE

Recommendation 1 - Enhance AMLC policies and procedures to reflect current practices for procuring, receiving, deploying, tracking, protecting, replacing, and disposing of IT assets.

Management Decision: Concur

The CIO, shortly after his arrival in November 2015, initiated a full review of all CIOO policies and procedures to ensure they were current and consistent with current operations. During the time of the audit, the circulars, policies, and work instructions related to the asset lifecycle were being revised and many were within their formal review process with the Division of Administration. FDIC Circulars 1380.1, 1380.2, and 1380.3, as well as DIT Policies 05-006 and 11-006, are currently under review and preparing for final signature.

Circular 1380.8 - Safeguarding Information Technology (IT) Hardware

Circular 1380.8 was sent out for DIT comment on May 26, 2016. It was sent out for corporate review by DOA on August 29, 2016. The corporate review completed on 5/1/2017and DOA delivered the circular to DIT to begin routing and obtaining signatures.

- Replaces and supersedes Circular 1380.1 - Assignment of FDIC Information Technology Hardware Assets and 1380.3 - Safeguarding FDIC Information Technology (IT) Hardware.

Circular 1380.2 - FDIC Information Technology (IT) Asset Management Life Cycle Program

DIT review of Circular 1380.2 began on May 30, 2016. It was sent out for corporate review by DOA on October 13, 2016. The Corporate review completed on 5/1/2017 and DOA delivered the circular to DIT to begin routing and obtaining signatures on 5/1/2017.

DIT Policy 05-006 - Policy on IT Asset Management Life Cycle

This policy is pending signoff within the CIOO.

DIT Policy 11-006 – Policy on Media Sanitization and Destruction

This policy is pending signoff within the CIOO.

Corrective Action:

Upon final corporate and CIOO approval, publish the identified relevant FDIC IT policies pertaining to the asset management lifecycle.

Estimated Completion Date: 10/6/2017

2

Corporation Comments

Recommendation 2 - Develop procedures for using the Technology Refresh Schedule as part of the procurement process and resolving open orders that have not been received for an extended period of time.

Management Decision: Concur

At the time of the evaluation, the FDIC shared with the IG the various Remedy reports that were developed to resolve open orders that had not been received for an extended period of time, including, but not limited to, the *On Order Report*, the *New Equipment Report*, and the *Timeliness of Securing Received Goods Report*. Excessively aged open orders on the *On Order Report* were the result of a known deficiency in Remedy that, without maintenance could not be addressed. That system has been replaced with Service Now, which does not have this deficiency. Further, the *On Order Report* (in ServiceNow) is currently reviewed by federal staff and contractors at the weekly Asset/Procurement meeting and orders over 30 days old are referred to the applicable Oversight Manager for action.

Corrective Action:

The FDIC will formalize and document the Technology Refresh planning procedures including considerations for the Enterprise Architecture and budget. The FDIC will also document how the Technology Refresh schedule is leveraged in the procurement process.

Estimated Completion Date: 8/4/2017

Recommendation 3 - Evaluate inventory timeframes to ensure they provide timely information about an asset's location.

Management Decision: Concur

The FDIC uses various tools including the new EAMS, mobile device management and automated patching tools to detect equipment usage and location. The FDIC evaluates the scope and inventory timeframe using these tools based upon last inventory date and technology refresh underway. Revised FDIC Circular 1380.2 and CIOO Policy 05-006 reflect *generalized* timeframes for hardware inventories. The revisions to the circular and policy address current mechanisms and frequencies associated with inventories.

Corrective Action:

The FDIC will issue Circular 1380.2 - FDIC Information Technology (IT) Asset Management Lifecycle Program and CIOO Policy 05-006, and will develop standard operating procedures (SOPs) for conducting sampling and data analysis for asset records. Deficiencies identified through sampling will be escalated to responsible asset custodians for remediation. In addition, where possible, the FDIC will conduct spot inventories and cycle counts in between physical inventories to validate that system data accurately reflects asset location.

Estimated Completion Date: 10/6/2017

Corporation Comments

Recommendation 4 - Establish procedures to ensure that separated employees have returned all assets assigned to them in EAMS as part of the pre-exit clearance process.

Management Decision: Concur

Departing employee's equipment is retrieved by their Supervisor or Client Services Section (CSS).

Corrective Action:

The FDIC CSS will establish a procedure to ensure that within 7 days of an employee's departure that EAMS has been updated accordingly. CSS will generate and review a report every week to measure compliance with this new procedure.

Estimated Completion Date: 8/4/2017

Recommendation 5 - Establish controls in EAMS that ensure adequate segregation of duties among individuals responsible for managing IT assets.

Management Decision: Concur

The FDIC notes that there is no order function that commits funds through ServiceNow; nothing can be purchased via ServiceNow. Warranted ASB Contracting Officers commit funding, and therefore make the "purchase," through NFE. The order details entered in ServiceNow are merely an administrative data entry "copy" for asset management purposes. While it is not feasible for a ServiceNow system user to purchase, order and receive equipment, the FDIC management believes that it is in the best interest of the Corporation to create new receiving roles and monitor the separation of the ordering and receiving roles which serves to strengthen the IT asset management program.

Corrective Action:

With the out-of-the-box functionality in ServiceNow, the procurement roles grant receiving access. Receiving access has been removed from the *procurement_admin* role and been included in the new standalone receiving roles of *fdic_receiving_user* and *fdic_receiving_admin*[1].

There is a management control in the FDIC access management system (IAMS) that requires several layers management approvals to ensure that the same person does not receive a procurement role and a receiving role in ServiceNow.

[1] FDIC Receiving User – this user is allowed to receive a procured line item and has access to the "Received button" on the PO. FDIC Receiving Administrator – same access as the FDIC Receiving User, but also can access the button "Refused on PO Line Item."

Corporation Comments

The FDIC will develop a procedure to regularly monitor system access for verification of roles segregation which will serve as a detective control.

Estimated Completion Date: 8/4/2017

Recommendation 6 - Review metrics used for data accuracy and timeliness of removing assets from end-of-life status.

Management Decision: Concur

Corrective Action:

The FDIC Asset Manager will review current inventory reports and will confer with custodial owners to help identify surplus IT equipment and to process retired assets more expeditiously.

Estimated Completion Date: 8/4/2017

Recommendation 7 - Establish a process for conducting data reliability reviews of key data elements within EAMS to ensure accuracy and completeness.

Management Decision: Concur

Corrective Action:

The FDIC Asset Manager will establish a procedure for conducting data reliability reviews using, as often as possible, automated means and reports.

Asset custodial owners will be responsible for conducting the reviews and correcting deficiencies and updating the system as needed.

Estimated Completion Date: 8/4/2017

Recommendation 8 - Establish means for holding DIT and Contractor staff more accountable for ensuring that EAMS data are accurate and complete.

Management Decision: Concur

Corrective Action:

The FDIC CSS will develop controls to routinely assess the level of data accuracy and completeness for the IT hardware asset data entered and edited by DIT federal staff.

The asset management team will review the ISC-3 contract and determine how compensation is tied to accurate and complete data maintenance. If a contract

Corporation Comments

modification is needed, the CIOO will work with GSA to implement the contract modification.

Additionally, CIOO Supervisors will evaluate the asset custodian's management of assets in the twice yearly Performance Management & Recognition (PMR) review.

Estimated Completion Date: 10/6/2017

Recommendation 9 - Improve IT asset management reporting to obtain reliable information that is timely and useful in managing the AMLC.

Management Decision: Concur

The FDIC uses various tools including the new EAMS, mobile device management and automated patching tools to detect equipment usage and location.

Corrective Action:

Prior to the completion of the evaluation fieldwork, the FDIC migrated to a new EAMS and both FDIC and contractor staff developed reports to monitor compliance with asset lifecycle policies on a monthly basis.

The FDIC will develop and implement new reports to inform and enhance asset management decisions to include, but not limited to, using EAMS data to help make management decisions about Technology Refresh.

Estimated Completion Date: 10/6/2017

Any questions regarding this response should be directed to Kim Farrell at (703) 516-5101.

cc: James Anderson, Acting Deputy Director, DOF, Corporate Management Control
Russell G. Pittman, Director, DIT
Isaac Hernandez, Deputy Director, DIT, Infrastructure Services Branch
Brian Aaron, Acting Deputy Director, DIT, Business Administration Branch
Rack D. Campbell, Chief, DIT, Audit and Internal Control

Summary of the Corporation's Corrective Actions

This table presents corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved: [a]Yes or No	Open or Closed[b]
1	During the evaluation, the Chief Information Officer Organization (CIOO) and DIT were revising AMLC-related circulars, policies, and work instructions. Upon final corporate and CIOO approval, these revised circulars and policies will be published.	October 6, 2017	$0	Yes	
2	The FDIC will formalize and document the Technology Refresh planning procedures, including considerations for the Enterprise Architecture and budget. The FDIC will also document how the Technology Refresh schedule is leveraged in the procurement process.	August 4, 2017	$0	Yes	
3	The revised Circular 1380.2 and CIOO Policy 05-006 will reflect generalized timeframes for hardware inventories and current mechanisms and frequencies associated with inventories. The FDIC will also develop standard operating procedures for conducting sampling and data analysis for asset records. In addition, where possible, the FDIC will conduct spot inventories and cycle counts in between physical inventories to validate that system data accurately reflect asset location.	October 6, 2017	$0	Yes	
4	The FDIC Client Services Section (CSS) will establish a procedure to ensure that within 7 days of an employee's departure, EAMS has been updated accordingly. CSS will	August 4, 2017	$0	Yes	

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved: [a]Yes or No	Open or Closed[b]
	generate and review a report every week to measure compliance with this new procedure.				
5	The FDIC noted that there is a management control in the new EAMS that requires management approvals to ensure that a user is not assigned a procurement role and a receiving role in EAMS. The FDIC will develop a procedure to regularly monitor system access for verification of role segregation which will serve as a detective control.	August 4, 2017	$0	Yes	
6	The FDIC Asset Manager will review current inventory reports and will confer with custodial owners to help identify surplus IT equipment and process retired assets more expeditiously. We also confirmed with DIT that it will review the 80 percent key contract performance indicator for EAMS data accuracy.	August 4, 2017	$0	Yes	
7	The FDIC Asset Manager will establish a procedure for conducting data reliability reviews using, as often as possible, automated means and reports. Asset custodial owners will be responsible for conducting the reviews, correcting deficiencies, and updating EAMS.	August 4, 2017	$0	Yes	
8	The FDIC CSS will develop controls to routinely assess the level of data accuracy and completeness for the IT hardware asset data entered and edited by DIT federal staff. The asset management team will review the infrastructure services	October 6, 2017	$0	Yes	

Summary of the Corporation's Corrective Actions

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved: [a]Yes or No	Open or Closed[b]
	contract and determine how compensation is tied to accurate and complete data maintenance. If a contract modification is needed, the CIOO will work with the General Services Administration to implement the contract modification. Additionally, CIOO Supervisors will evaluate the asset custodian's management of assets in the twice yearly Performance Management & Recognition review.				
9	The FDIC will develop and implement new reports to inform and enhance asset management decisions including, but not limited to, using EAMS data to help make management decisions about Technology Refresh.	October 6, 2017	$0	Yes	

[a] Resolved – (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.