Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-13-007

The FDIC's Controls over Business Unit-Led Application Development Activities

September 2013

Office of Inspector General

Executive Summary

The FDIC's Controls over Business Unit-Led Application Development Activities

Report No. AUD-13-007
September 2013

Why We Did The Audit

Business unit-led application development generally refers to the creation or enhancement of information technology (IT) solutions where the development is performed under the direction of an FDIC business division or office (referred to herein as a business unit), rather than the FDIC's Division of Information Technology (DIT). In our most recent information security program evaluation report required by the Federal Information Security Management Act of 2002, we noted that such development activity presents risk because it generally occurs outside of formal risk management and IT governance processes. Accordingly, we decided to review this area in more detail.

The objectives of the audit were to identify key risks associated with the FDIC's business unit-led application development activities and to determine the extent to which controls have been established to mitigate those risks.

Background

Within the FDIC, DIT has primary responsibility for managing the FDIC's IT program and operations, including the development and enhancement (collectively referred to herein as development) of applications. The Director, DIT, reports to the FDIC's Chief Information Officer (CIO), who has corporate-wide strategic responsibility for IT governance, investments, program management, and information security. DIT follows formal risk management and IT governance processes when developing applications. Such processes include the Rational Unified Process systems development life cycle (SDLC) methodology and corporate policies and procedures that address such things as the enterprise architecture, data management, information security, privacy, configuration management, and quality assurance. In addition, the FDIC has established various governance bodies, such as the Capital Investment Review Committee and the CIO Council, to provide oversight and control of application development initiatives that meet certain criteria.

The FDIC's business units also engage in application development activity and, in some cases, have established specialized IT support service units to perform the development work. Business unit-led application development ranges from the building of simple applications with only a few users to complex applications with hundreds of users. Consequently, the cost of the applications can vary from a few thousand dollars to over $1 million. Such development can also involve creating new data or collecting sensitive information, such as personally identifiable information, that is used to support important business functions, such as large bank supervision, the marketing of failing banks, and human resources management.

Business units fund their application development activities through their operational budgets. However, there is no FDIC policy requirement for business units to track or report the costs of their development activities to FDIC management officials, and business units did not do so. As a result, we were unable to determine the total amount spent on business unit-led application development at the FDIC. The majority of the FDIC's business unit-led application development occurs within the Division of Resolutions and Receiverships and the Division of Risk Management Supervision.

In January 2013, DIT began hosting a series of meetings with division and office representatives to discuss issues associated with business unit-led application development and to develop a corporate policy and supporting guidance in this area. The corporate policy and guidance is intended to provide, among other things, criteria for identifying application development efforts that are appropriate for business unit-led development, the IT governance processes that should apply, and the project activities involved.

Audit Results

Business unit-led application development provides the FDIC's divisions and offices with the flexibility to rapidly develop and deploy IT solutions to support information analysis and management decision-making. However, this type of development also presents risk because it has generally occurred outside of the FDIC's established risk management framework and IT governance processes that are designed to ensure internal controls are addressed. Key risks associated with the FDIC's business unit-led application development activities that we identified during the audit include not:

- recording the applications in the FDIC's information systems inventory, thereby limiting the FDIC's assurance that the applications are subject to appropriate risk management procedures and oversight;

- subjecting development projects to appropriate IT governance processes, thus reducing the FDIC's assurance that IT investment decisions are consistent with corporate and division goals and priorities; and

- establishing appropriate SDLC standards, therefore limiting the FDIC's assurance that applications are properly designed and tested, systems documentation is adequate, and information security and privacy requirements are addressed.

We identified certain controls that were established by the FDIC's business units that mitigated, to some extent, the risks described above. Such controls included SDLC guidelines and procedures to guide certain application development activities and committees to provide oversight of IT activities. However, control improvements are needed in all three areas.

Recommendations and Corporation Comments

The FDIC's planned corporate policy and related guidance on business unit-led application development can promote a better understanding of this type of development activity and the associated risk management procedures and IT governance processes that should apply. Our report contains three recommendations addressed to the FDIC's Acting CIO that are intended to assist the FDIC with those ongoing efforts. In general, the recommendations are aimed at establishing appropriate policies, procedures, and guidance to ensure that applications are recorded in the Corporation's information systems inventory, when appropriate; that business units have appropriate IT governance processes and SDLC standards; and that existing applications comply with FDIC security policies. The Acting CIO provided a written response, dated September 6, 2013, to a draft of the report. In the response, the Acting CIO concurred with all three of the report's recommendations and described ongoing and planned actions to address the recommendations.

Contents

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

Office of Audits and Evaluations
Office of Inspector General

DATE: September 11, 2013

MEMORANDUM TO: Martin D. Henning
Acting Chief Information Officer

/Signed/
FROM: Stephen M. Beard
Deputy Inspector General for Audits and Evaluations

SUBJECT: *The FDIC's Controls over Business Unit-Led Application Development Activities* (Report No. AUD-13-007)

This report presents the results of our performance audit of the FDIC's controls over business unit-led application development[1] activities. Although the FDIC has not yet adopted a formal definition of business unit-led application development, the term generally refers to the creation or enhancement of information technology (IT) solutions where the development is performed under the direction of an FDIC business division or office (referred to herein as a business unit), rather than the Division of Information Technology (DIT).

The objectives of the audit were to identify key risks associated with the FDIC's business unit-led application development activities and to determine the extent to which controls have been established to mitigate those risks. Our work included interviewing officials in DIT and selected FDIC business units and reviewing available documentation for a non-statistical sample of four applications.[2] Two of these applications were developed by the Division of Resolutions and Receiverships (DRR), and two were developed by the Division of Risk Management Supervision (RMS). We reviewed these four applications to obtain an understanding of the associated development practices. We did not assess whether the applications were properly designed or controls were properly implemented. We reviewed one additional application developed by DIT for reference purposes. The results of this audit will assist our office in fulfilling its information security program evaluation and reporting responsibilities under the Federal Information Security Management Act of 2002 (FISMA).

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report includes additional details on our objectives, scope, and methodology; Appendix 2 contains a glossary of key terms;

[1] Terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Terms*.
[2] A non-statistical sample cannot be projected to the population. See Appendix 1 for a complete description of our sample selection and sampling methodology, including a Table listing the applications we reviewed.

Appendix 3 contains a list of acronyms and abbreviations; Appendix 4 contains the Corporation's comments on this report; and Appendix 5 contains a summary of the Corporation's corrective actions.

Background

Within the FDIC, DIT has primary responsibility for managing the FDIC's IT program and operations, including the development and enhancement (collectively referred to herein as development) of applications. The Director, DIT, reports to the FDIC's Chief Information Officer (CIO), who has corporate-wide strategic responsibility for IT governance, investments, program management, and information security.[3] DIT follows formal risk management and IT governance processes when developing applications. Such processes include the Rational Unified Process® (RUP)® systems development life cycle (SDLC) methodology and corporate policies and procedures that address such things as the enterprise architecture (EA), data management, information security, privacy, configuration management, and quality assurance. In addition, the FDIC has established various governance bodies, such as the Capital Investment Review Committee (CIRC) and the CIO Council, to provide oversight and control of application development initiatives that meet certain criteria.[4] As of June 30, 2013, the CIRC was overseeing an application development budget of $18.45 million for 2013, and the CIO Council was overseeing an application development budget of $20.99 million for 2013.

The FDIC's business units also engage in application development activity and, in some cases, have established specialized IT support service units to perform the development work.[5] According to the *FDIC Business Technology Strategic Plan: 2013-2017*, this type of development activity provides the FDIC with the agility to address immediate business needs with minimal resource demands on DIT. Business unit-led application development ranges from the building of simple applications with only a few users to complex applications with hundreds of users. Consequently, the cost of the applications can vary from a few thousand dollars to over $1 million. Such development can also involve creating new data or collecting sensitive information, such as personally identifiable information (PII), that is used to support important business functions, such as large bank supervision, the marketing of failing banks, and human resources management.

[3] Prior to July 23, 2013, the positions of DIT Director and CIO were held by the same individual. On that date, the FDIC implemented an organizational change separating these roles to enhance the IT area and address a wide range of increasing IT security risks in the current global environment.

[4] The CIRC is responsible for approving and overseeing all capital investment projects, including IT projects, with total investment budgets of $3 million or more or that are deemed to have a significant corporate impact, regardless of cost. The CIO Council is responsible for approving and monitoring various types of IT projects, including application development projects.

[5] FDIC business units, rather than DIT, performed ongoing maintenance for the business unit-developed applications that we selected for review. Maintenance includes, among other things, changes to production software to correct known problems and to prevent anticipated problems or inefficiencies.

Business units fund their application development activities through their operational budgets. FDIC policy directives do not require business units to track or report the costs of their development activities to FDIC management officials, and no such costs were being tracked and reported. As a result, we were unable to determine the total amount spent on business unit-led application development at the FDIC.

Divisions Engaged in Business Unit-Led Application Development

Based on our discussions with DIT and business unit personnel, we determined that the majority of business unit-led application development occurs within DRR and RMS. Within DRR, the Business Information Services (BIS) section in Dallas, Texas, and the Business Program Management (BPM) section in Arlington, Virginia, perform the development. Within RMS, the Business Analysis and Decision Support (BADS) section in Washington, D.C., and personnel in the Regional Office Management Information Groups (ROMIGs) perform the development. A notable difference between DRR and RMS in their approach to application development is that DRR generally engages contractors to perform the work, while RMS uses in-house personnel. In addition, DRR was working to centralize its IT operations (including application development) by consolidating BIS and BPM, while RMS' development activities remain decentralized. At our request, DRR and RMS compiled listings of the applications they had developed (or were working to develop). DRR's listing contained 23 applications and RMS' listing contained 53 applications. Most of these applications were developed using Oracle® Application Express (APEX) or Microsoft® Access.[6]

To help mitigate the risks associated with business unit-led application development, DRR and RMS each entered into formal agreements with DIT that defined certain roles and responsibilities and other expectations regarding the use of one particular software development tool—APEX. Specifically, RMS and DIT executed the *FDIC Governance Plan for Implementation, Use and Support of Application Express (APEX) for DSC,* dated December 2009 (RMS APEX Governance Plan),[7] and DRR and DIT executed a *Memorandum of Understanding for Use of Application Express (APEX) by the Division of Resolutions and Receiverships (DRR),* dated December 2010 (DRR APEX MOU). In general, these agreements contemplate the use of APEX for the rapid development and deployment of simple applications, reports, and forms. No similar agreements were executed with other divisions or offices or for other software development tools.

Ongoing Efforts to Address Risks Associated with Business Unit-Led Application Development

DIT's 2012 Assurance Statement identifies business unit-led development and/or procurements of IT systems, solutions, and/or processes outside of established IT

[6] FDIC business units may use other FDIC-approved IT development tools, such as the Statistical Analysis System (SAS) software, to develop applications. For security reasons, our report does not include the names of the applications developed by RMS and DRR.

[7] Subsequent to the execution of this document, the FDIC's Division of Supervision and Consumer Protection (DSC) was reorganized into RMS and the Division of Depositor and Consumer Protection.

governance and control processes as a non-material challenge for 2013. The assurance statement explains that modern organizations, including the FDIC, are challenged with balancing end-user flexibility in the development of business products with the robust IT security and compliance controls necessary to safeguard the often sensitive data that those products utilize. According to the assurance statement, business unit-led application development can create an environment that supports critical business processes, but these IT activities often do not satisfy FDIC's requirements for control, documentation, security, and reliability. The assurance statement adds that the ability of business units to create their own applications outside of formal FDIC IT processes creates significant security concerns and additional demands on DIT and business unit resources.

In our most recent information security program evaluation report required by FISMA, we noted that development activity in FDIC's business units presents risk because the development occurs outside of formal risk management and IT governance processes.[8] We recommended that the CIO coordinate with the FDIC's business divisions and offices to develop criteria that define when business unit-led application development efforts should be incorporated into the FDIC's risk management framework and IT governance processes. The CIO concurred with the recommendation and agreed to submit a corporate policy and supporting guidance to the FDIC's Division of Administration, which has responsibility for issuing corporate policy directives, by July 1, 2013.[9]

In January 2013, DIT began hosting a series of meetings with division and office representatives to discuss issues associated with business unit-led application development and to develop a corporate policy and supporting guidance in this area. During the interdivisional meetings, it was recognized that:

- a better understanding of what constitutes an application for purposes of applying risk management procedures and IT governance processes is needed.

- the FDIC has a duty to ensure that all business unit-led application development efforts adhere to certain established practices and standards to ensure the solutions meet agency business needs, are consistent with relevant risk management policies, and comply with applicable federal laws and FDIC policies and guidelines (including those related to information security).

- the level of risk management and IT governance applied to application development should be commensurate with the risks and complexities of the development efforts. In many cases, such as when business units develop simple spreadsheets, databases, and reports, minimal risk management requirements should apply.

[8] *Independent Evaluation of the FDIC's Information Security Program—2012* (Report No. AUD-13-003, dated November 5, 2012).
[9] DIT management subsequently extended this date to October 1, 2013.

The corporate policy and related guidance under development is intended to provide, among other things, criteria for identifying application development efforts that are appropriate for business unit-led development, the IT governance processes that should apply, and the project activities (including security activities) involved.

Audit Results

Business unit-led application development provides the FDIC's divisions and offices with the flexibility to rapidly develop and deploy IT solutions to support information analysis and management decision-making. However, this type of development also presents risk because it has generally occurred outside of the FDIC's established risk management framework and IT governance processes that are designed to ensure internal controls are addressed. Key risks associated with the FDIC's business unit-led application development activities that we identified during the audit include not:

- recording the applications in the FDIC's information systems inventory, thereby limiting the FDIC's assurance that the applications are subject to appropriate risk management procedures and oversight;

- subjecting development projects to appropriate IT governance processes, thus reducing the FDIC's assurance that IT investment decisions are consistent with corporate and division goals and priorities; and

- establishing appropriate SDLC standards, therefore limiting the FDIC's assurance that applications are properly designed and tested, systems documentation is adequate, and information security and privacy requirements are addressed.

We identified certain controls that were established by the FDIC's business units that mitigated, to some extent, the risks described above. Such controls included SDLC guidelines and procedures to guide certain application development activities and committees to provide oversight of IT activities. However, control improvements are needed in all three areas.

As discussed earlier, the FDIC was working to develop a corporate policy and related guidance that is intended to promote a better understanding of what constitutes business unit-led application development and the associated risk management procedures and IT governance processes that should apply. Such policy and guidance is intended to be commensurate with the risks and complexities of the development efforts. Our report includes three recommendations intended to further the FDIC's ongoing efforts to establish appropriate policies, procedures, and guidance over these activities.

Risks and Controls Related to Business Unit-Led Application Development

We identified key risks associated with the FDIC's business unit-led application development activities by reviewing relevant internal FDIC documents, such as DIT's 2012 Assurance Statement and the *FDIC Business Technology Strategic Plan: 2013-2017*; interviewing DIT and business unit personnel; gaining an understanding of the FDIC's approach to this type of development; and researching industry guidance. We determined the extent to which controls were established to mitigate those key risks by reviewing FDIC policies, procedures, and guidance, the roles and responsibilities of IT governance bodies, and other relevant control activities; interviewing DIT and business unit personnel; and reviewing the FDIC's development practices for a sample of applications. A description of these key risks and controls, as well as actions that the FDIC can take to further mitigate the risks, follows.

Information Systems Inventory

FISMA requires federal agencies, including the FDIC, to provide risk-based information security protections for all of their information systems (including applications). Establishing and maintaining a current, accurate, and complete inventory of information systems can support agency efforts to address this risk management requirement and to determine where the agency's information security program should direct its resources. In addition, the inventory can facilitate application portfolio analysis and reporting in support of IT governance processes and the EA. The FDIC currently uses the EA Repository (EA-Rep) as an inventory tool to record important information about the FDIC's applications, such as key business, technical, and contractor contacts, number of users, security category, privacy impact, mission criticality, and supporting hardware and software resources.

A key risk associated with business unit-led application development is that applications may not be recorded in the FDIC's information systems inventory, thereby limiting the FDIC's assurance that such applications are subject to appropriate risk management procedures and oversight.[10] The inventory helps the FDIC ensure that business unit-led applications containing sensitive or privacy information are properly identified as such and aggregated under a general support system (GSS) or major application for purposes

[10] According to FISMA, information security protections should be commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA also requires agencies to maintain an inventory of major information systems (44 U.S.C. § 3505(c)). The FDIC uses application information in the EA-Rep to satisfy that requirement.

of applying security oversight.[11] Such oversight includes testing and evaluation of security controls, authorizations to operate, and acceptance of residual risk.

On December 15, 2010, DIT issued Policy Number 10-004, *Policy on Maintaining the Enterprise Architecture Repository (EA-REP).* The policy establishes responsibilities for ensuring that information in the EA-Rep is accurate, complete, and up-to-date. However, the policy is targeted to DIT employees and the systems and applications that are developed or supported by DIT, and does not specifically reference applications developed by the FDIC's business units. The RMS APEX Governance Plan requires that all APEX applications developed by RMS be recorded in the EA-Rep. The DRR APEX MOU does not contain this specific requirement but does require DRR to ensure compliance with DIT policies and standards.

We reviewed the EA-Rep and found that it did not contain APEX applications developed by DRR's BIS or RMS. In addition, the EA-Rep did not contain one of the two RMS applications in our sample that was developed with Microsoft® Access.[12] Although the EA-Rep contained APEX applications developed by DRR's BPM, we noted that those applications, as well as APEX applications developed by DIT, were not consistently identified as APEX applications in the EA-Rep. These inconsistencies limited the FDIC's assurance that the population of APEX applications recorded in the EA-Rep was complete. Further, neither DRR nor RMS maintained a single authoritative inventory of the applications they developed.[13]

The FDIC can mitigate the risks described above by including language in its planned policy on business unit-led application development that requires business units to ensure their applications are recorded in the FDIC's information systems inventory, when appropriate.

IT Governance

Effective IT governance processes help ensure that management's expectations are met and that relevant risks are mitigated. The FDIC's formal IT governance structure consists of governance bodies, including the CIRC and CIO Council; corporate policies, procedures, and guidance; and the *FDIC Business Technology Strategic Plan: 2013–2017*. At the business unit level, RMS established the RMS IT Portfolio Review Committee (PRC) in April 2004 to advise RMS' executive management on the selection

[11] FDIC security plans for minor applications identify the GSS or major application that provides the majority of security controls for the minor application. Security testing of minor applications is then covered by (or "aggregated under") the security testing of the associated GSS or major application. This process of aggregating minor applications under a GSS or major application represents a cost-effective alternative to conducting separate security procedures for individual applications. However, the process requires that DIT be aware of the minor applications, and the inventory facilitates this awareness.

[12] We also identified two Microsoft® Access applications supported by DRR's BPM that were not in the EA-Rep.

[13] DRR maintained an inventory of APEX applications developed by DRR BIS on a SharePoint site. Other lists of DRR applications were also stored on DRR's Intranet site.

and monitoring of important new IT development projects. In addition, DRR established the DRR Systems Governance Board (SGB) in October 2011 to oversee its IT activities, including the approval of rapid application development projects and the resources needed to support those projects.

A key risk associated with business unit-led application development is that it may not be subject to appropriate IT governance processes, thus reducing the FDIC's assurance that IT investment decisions are consistent with corporate and division goals and priorities. For example, business units may design applications that duplicate existing functionality or data, resulting in unnecessary costs and inefficiencies. Inadequate IT governance processes may also result in unexpected delays to IT projects that have been approved through formal processes if DIT needs to divert resources to address unanticipated issues with applications developed by business units.

An important component of IT governance is the formal review and approval of development proposals to ensure they satisfy corporate and division goals and priorities. Neither of the development proposals for the two DRR applications that we selected for review had been reviewed or approved by the SGB because it was established after the applications were initially developed. However, DRR officials informed us that the SGB now reviews business unit-led development proposals. We were provided with a template used to prepare such development proposals and an example of SGB meeting minutes showing that the SGB had discussed the justification and level of effort for a more recent application development effort. A DRR official informed us that the division was working to document its end-to-end IT governance processes.

With respect to the two RMS applications that we reviewed, an RMS official informed us that the PRC did not review one of the applications because it was developed with APEX and the PRC does not review APEX development proposals.[14] RMS officials thought that the remaining application may have been reviewed by the PRC but were not able to locate any documentation pertaining to a PRC review of the application. In addition, because the PRC did not maintain meeting minutes, we were unable to determine the extent to which RMS application development efforts were reviewed and discussed by the PRC. An RMS official informed us that RMS plans to expand the responsibilities of the PRC to include additional oversight of business unit-led application development projects.

The agreements between DRR, RMS, and DIT on APEX were intended to help guide and control APEX development activities. The agreements noted the need for collaboration and communication between DIT and the divisions to ensure effective development. However, DIT, DRR, and RMS officials informed us that communication between the business units and DIT regarding the use of the APEX tool was not always effective. As a result, DIT was not aware of the extent to which APEX development activities were taking place in the business units.

[14] Of the 53 applications that RMS developed (or were working to develop), 11 were APEX applications.

Another important component of IT governance is the formal management decision to authorize the deployment of an application into the production environment based on an independent verification that all required application development activities have taken place. DRR had various written guidelines[15] and work products pertaining to the review and authorization of its application deployment activities. However, RMS had not developed written guidelines or work products that addressed those activities. An RMS official informed us that applications and reports that are expected to become permanent or reach a significant user base are tested by developers and pilot users, and receive RMS management approval before they are placed into production.

Cost management, including comparing projected costs and benefits to actual results, is also a fundamental tenet of IT governance. As previously discussed, there is no FDIC policy requirement for business units to track and report the costs of their application development activities to FDIC management officials. However, at our request, DRR officials estimated that about $8.3 million in contractor resources were expended to develop and maintain 14 APEX applications during the period September 2010 through June 2013.[16] Notably, estimated contract expenditures for 4 of the 14 applications exceeded $1 million each, the highest of which was $1.54 million. RMS used in-house personnel, rather than contractors, to develop its APEX applications. RMS did not track the in-house costs of its application development efforts. Further, although DRR's BIS estimated the cost of in-house personnel involved in developing individual APEX applications, DRR's BPM did not. Because DRR and RMS funded application development through their operational budgets, the costs were not subject to CIO Council oversight.

The FDIC can strengthen its controls over business unit-led application development activities by including language in the planned corporate policy requiring business units to develop and document appropriate IT governance processes. Such processes should address the review and approval of development proposals, the decision-making process to authorize the deployment of applications into the production environment, and the tracking and reporting of application development costs. Such processes should also be scaled to the risk and complexity of the development activities involved so as not to unduly impede the ability of business units to address low risk (as determined by the significance of the functionality and sensitivity of the data being processed and maintained) reporting, analytical, and automation needs.

[15] The guidelines included the *FDIC Business Information Systems (BIS) Configuration Management – Change Control Guide Version 1.0*, dated November 30, 2011; *the Business Information Systems (BIS) Configuration Management Plan, Version 1.0*, dated September 25, 2012; and the *FDIC PRR Configuration Management Plan Version: 1.0*, dated December 5, 2012.

[16] At the close of our audit, we were informed that DRR planned to procure significant contractor support for business unit-led application development, maintenance, and operational support as well as expert resources in WebFocus.

Systems Development Life Cycle Standards

The SDLC is the process of managing information systems from initiation, analysis, design, implementation, and maintenance, to disposal. The National Institute of Standards and Technology (NIST) recommends that federal agencies have a documented and repeatable SDLC policy and guideline that support the agencies' business needs and complement their unique culture.[17] In addition, our review of industry research in this area indicates that some leading organizations are creating processes to set standards for sourcing, developing, and deploying IT, to be applied throughout the enterprise. These organizations then assess and recognize (through training and accreditation) staff outside of the formal IT organization that need or want to have the necessary capabilities and approach to meet those standards. According to the research, this approach provides CIOs with increased assurance that appropriate standards of agility, architectural compliance, maintainability, and security are followed throughout the organization.

DIT Policy Number 07-005, *Systems Development Life Cycle*, states that DIT has adopted a customized RUP® SDLC methodology to meet the FDIC's specific requirements for application development. RUP® contains process roadmaps that provide step-by-step activities for development projects of varying size, type, risk, and complexity. Applications developed by the FDIC's business units are not required to follow RUP®, and DRR and RMS have developed their own approach to application development. In addition, both divisions have an information security manager (ISM) who is responsible for assisting application development teams in addressing information security and privacy requirements.

A key risk associated with business unit-led application development is that business units may not establish appropriate written SDLC standards, therefore limiting the FDIC's assurance that:

- applications are properly designed and tested to ensure they operate as intended,
- systems documentation is sufficient to support effective maintenance, and
- security and privacy requirements are addressed.

SDLC Standards

SDLC standards, which are defined through written procedures and guidelines and documented work products, provide an important control for ensuring that application development processes are repeatable, consistent, and disciplined and for reducing operational risk associated with changes in staff. Training can provide increased

[17] See NIST Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, dated October 2008. This publication helps address requirements in FISMA that federal agencies, including the FDIC, have policies and procedures to ensure that information security is addressed throughout the life cycle of their information systems.

assurance that SDLC standards are properly implemented. Although we did not include training within the scope of this audit, we did recommend in our 2012 information security program evaluation report that the CIO update the FDIC's IT security training plan to clarify the FDIC's approach for addressing the corporate-wide information security training needs of individuals with significant information security responsibilities. Such individuals can include business unit personnel engaged in application development. As described below, DRR and RMS had not developed a policy addressing SDLC standards for their business unit-led application development, established consistent written SDLC standards, or designated a standard repository to store their application code and software documentation.

In July 2011, DRR issued high-level SDLC guidance to supplement the DRR APEX MOU. Subsequently, in 2012, DRR's BPM and BIS separately developed informal SDLC guidelines. Although these guidelines were based on DIT's RUP® methodology, their content and level of specificity differed. Specifically, BPM's *Client Development Guidelines* defined key application development phases and activities, required work products, and roles and responsibilities, while BIS's *DRR SDLC - Rapid RUP*® provided more limited process guidance. In addition, neither of the guidelines adequately addressed procedures for documenting consideration and implementation (as necessary) of requirements pertaining to the EA and Section 508 accessibility.[18] Further, DRR officials informed us that the division had selected StarTeam® as its standard repository for storing business unit developed application code and software documentation.[19] DRR officials also informed us that they were working to develop formal SDLC guidelines to promote consistency in DRR's application development activities.

RMS did not have written SDLC guidelines to govern its application development activities. However, we noted that RMS developers had various documentation indicating certain change management and quality assurance testing activities had been performed prior to the deployment of the applications we reviewed. In addition, RMS stored its business unit-developed application code and software documentation on various shared drives or in StarTeam®. However, RMS had not formally designated a standard repository for storing this information.

The written agreements between DRR, RMS, and DIT regarding the use of APEX also provide some SDLC guidance. However, the agreements address only those applications

[18] See FDIC Circulars 1303.1, *FDIC Enterprise Architecture Program*, dated June 16, 2008, and 2711.1, *Electronic and Information Technology (EIT) Accessibility Pursuant to Section 508 of the Rehabilitation Act*, dated September 27, 2007. It is generally the responsibility of application developers in the business units to coordinate with DIT subject matter experts to ensure requirements pertaining to the EA and Section 508 are addressed. DIT personnel advised us that guidance was being developed to facilitate compliance with Section 508 requirements, as applicable, for all FDIC applications.

[19] DIT also uses StarTeam® as a repository of application code and software documentation (including copies of security and privacy-related work products).

developed with APEX and do not adequately address the development-related controls described in this report. Such controls include ensuring that:

- applications are designed to align with the FDIC's current and target EA;
- data duplication and redundant processes are mitigated to the extent possible;
- software components are uniquely identified, consistently stored, subject to appropriate version control and change control processes, and adequately tested and reviewed prior to implementation;
- applications are Section 508 compliant, that is, they are as accessible to persons with disabilities, including employees and members of the public, as they are for persons without disabilities; and
- applications are reviewed for sensitivity and that sensitive information is adequately protected from unauthorized access or modification.

Absent appropriate written SDLC standards to guide application development in the business units, there is an increased risk that applications will not be properly designed or tested as intended or that systems documentation will not be sufficient to support effective maintenance.

Information Security and Privacy

Important controls for ensuring that information security and privacy are integrated into applications include sensitivity assessments, privacy reviews, security planning, access control reviews, and separation of duties. FDIC Circular 1310.3, *Information Technology Security Risk Management Program,* dated July 6, 2005, states that all FDIC applications must undergo a sensitivity assessment to examine the sensitivity level of the information they process and determine their security category. This assessment is documented in an Application Security Assessment (ASA). The FDIC has also established policies and procedures requiring divisions and offices to complete a privacy questionnaire, referred to as a Privacy Threshold Analysis (PTA), whenever new systems or applications are developed or acquired. The PTA is used to determine whether a statutory Privacy Impact Assessment (PIA) is required.

In addition, Circular 1310.3 states that a security plan shall be developed and tested for all sensitive applications. Security plans provide an overview of the application or system security requirements and describe the controls that are planned or in place to meet those requirements. Further, FDIC Circular 1360.15, *Access Control for Information Technology Resources*, dated February 27, 2009, requires periodic reviews of access to ensure consistency with existing authorizations and current business needs. It also addresses the concept of separation of duties.

An ASA, PTA, and security plan were prepared for each of the two DRR applications that we selected for review. In addition, an ASA, PTA, and security plan were prepared for one of the two RMS applications that we reviewed. However, the ASA and security plan for this RMS application were drafted in late 2011, but not finalized, reviewed, and approved by the RMS ISM until May 2013, approximately 1 year after the application was placed into the production environment. The RMS ISM informed us that APEX applications and applications developed in the RMS regional offices are subject to ISM review only upon request by the development teams.[20] An ASA and PTA were not prepared for the remaining RMS application that we reviewed because the system manager was not aware of the policy requirements for these work products. We were informed that this application contains sensitive information. As a result, it may require a security plan depending on the results of an ASA, and/or a PIA depending on the results of a PTA.

As of the close of our audit, DRR officials had not provided ASAs or security plans for their APEX applications to DIT's Information Security and Privacy Staff (ISPS). DRR officials indicated that they were awaiting guidance from DIT's ISPS regarding the submission of these documents. RMS recently provided such work products to DIT's ISPS. DIT's ISPS uses information from these work products, along with the systems inventory, to help ensure that security for minor applications, including those developed by the FDIC's business units, is coordinated with the security oversight of GSSs and major applications. We noted that the aggregation of security plans to GSSs by DRR, RMS, and DIT was inconsistent for the four APEX applications that we reviewed, limiting the FDIC's assurance that these applications are subject to appropriate security oversight.[21]

Further, DRR had established written access control procedures that addressed access reviews for all of the division's applications, including those developed under the division's direction. Although an RMS official provided us with a guideline and some examples of periodic access control reviews for one of our sampled applications, RMS had not established written access control procedures covering all their business unit-developed applications. Access control reviews involve periodically verifying that user accounts are properly authorized and confirming that specific permissions granted remain appropriate. Completing such reviews, which are consistent with the security principle of least privilege, provides assurance that users remain in appropriate roles and status and that only appropriate users have administrative access.

---

[20] According to the RMS ISM, an ASA, PTA, and security plan (if applicable) have been completed for 2 of the 11 APEX applications developed or under development by RMS. The RMS APEX Governance Plan does not specifically require the completion of an ASA, PTA, or security plan for RMS APEX applications. However, it does contain a general requirement that RMS complete and submit the security work products necessary to satisfy regulatory mandates.

[21] The two DRR applications we reviewed were primarily aggregated to the Enterprise Data Management GSS, and the RMS application was primarily aggregated to the Windows Server GSS. The DIT application was aggregated to the Midrange Servers GSS. The RMS APEX Governance Plan indicates that all APEX applications developed by RMS should be aggregated to the Enterprise Data Management GSS. The DRR APEX MOU does not contain guidance regarding aggregation.

Separation of duties in the context of systems development involves having different individuals performing key functions (e.g., programming and maintenance). Such a control is important for mitigating the risk of malevolent IT activities, improper program changes, and unauthorized access to sensitive information. We noted that DRR had established controls to restrict application development personnel from accessing the production environment. However, separation of duties for the two RMS applications we reviewed were not adequate because the personnel responsible for developing the application code were also responsible for transferring the code into, and had access to the code in, the production environment. We were also informed that RMS' APEX development and quality assurance activities were performed by developers in a pre-production environment on a production server that is separate from the application workspaces and data used for production.

The FDIC can achieve increased assurance that security and privacy requirements are addressed in business unit-led application development by establishing controls to address the issues described in this report.

Recommendations

We recommend that the Acting CIO:

1. Include language in the planned corporate policy on business unit-led application development that requires FDIC business units to:

    a) coordinate with DIT to ensure that applications developed by business units are recorded in the Corporation's information systems inventory, when appropriate; and

    b) develop written IT governance processes that address the review and approval of development proposals, the decision-making process for authorizing the deployment of applications to the production environment, and the tracking and reporting of application development costs.

2. Coordinate with FDIC business units involved in application development to establish appropriate written SDLC standards that are consistent with applicable laws, policies, and guidelines, and commensurate with the risks and complexity of their development activities.

3. Coordinate with DRR and RMS to ensure that existing applications developed under the divisions' direction comply with FDIC security policies pertaining to sensitivity assessments, privacy reviews, security plans, access control reviews, and separation of duties.

Corporation Comments and OIG Evaluation

The Acting CIO provided a written response, dated September 6, 2013, to a draft of this report. The response is presented in its entirety in Appendix 4. In the response, the Acting CIO concurred with all three of the report's recommendations and described ongoing and planned actions to address the recommendations.

A summary of the Corporation's corrective actions is presented in Appendix 5. The ongoing and planned actions are responsive to the recommendations, and the recommendations are resolved.

Objectives, Scope, and Methodology

Objectives

The objectives of the performance audit were to identify key risks associated with the FDIC's business unit-led application development activities and to determine the extent to which controls have been established to mitigate those risks.

We conducted this performance audit from January 2013 to July 2013 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

We identified key risks associated with the FDIC's business unit-led application development activities by reviewing relevant internal FDIC documents, interviewing DIT and business unit personnel, and researching industry guidance. We determined the extent to which controls were established to mitigate those key risks by reviewing relevant FDIC policies, procedures, and guidance, the role of IT governance bodies, and other relevant control activities; interviewing DIT and business unit personnel; and reviewing the FDIC's development practices for a sample of applications. Our work related to controls was limited to determining the extent to which policies, procedures, reports, IT governance bodies, and other relevant control activities were in place. We did not assess whether these controls were effectively implemented or operating as intended.

To achieve the audit objectives, we performed the following procedures:

- Interviewed personnel in RMS, DRR, DIT, the Division of Depositor and Consumer Protection, Division of Insurance and Research, Division of Finance, and Division of Administration who were involved with business unit-led application development to obtain their perspectives on relevant risks, controls, development practices, tools, and costs.

- Obtained an understanding of corporate and division-level policies[22] and procedural guidance related to application development by reviewing the following:

    - FDIC Circular 1303.1, *FDIC Enterprise Architecture Program*
    - FDIC Circular 1301.3, *Enterprise Data Management Program*
    - FDIC Circular 1310.3, *Information Technology Security Risk Management Program*

[22] In general, these FDIC policies are founded on legislative requirements or on standards and guidance issued by NIST.

- FDIC Circular 1360.8, *Information Security Categorization*
- FDIC Circular 1320.4, *FDIC Software Configuration Management Policy*
- FDIC Circular 1360.18, *FDIC Software Quality Assurance Policy*
- FDIC Circular 2711.1, *Electronic and Information Technology (EIT) Accessibility Pursuant to Section 508 of the Rehabilitation Act*
- DIT Policy Number 07-005, *Policy: Systems Development Life Cycle*
- DIT Policy Number 10-004, *Policy on Maintaining the Enterprise Architecture Repository (EA-REP)*
- *FDIC Governance Plan for Implementation, Use and Support of Application Express (APEX) for DSC*
- *Memorandum of Understanding for Use of Application Express (APEX) by the Division of Resolutions and Receiverships (DRR)*
- DRR *Business Program Management Section (BPMS) Client Development Guideline*
- DRR Business Information System's *DRR SDLC – Rapid RUP®*
- *DRR APEX Software Development* process guidance

- Reviewed internal FDIC documents, such as the *FDIC Business Technology Strategic Plan 2013-2017* and DIT's 2012 Assurance Statement submitted pursuant to the Federal Managers' Financial Integrity Act,[23] the Chief Financial Officers Act of 1990,[24] and FDIC Circular 4010.3, *FDIC Enterprise Risk Management Program*, for information about risks related to business-unit led application development.

- Reviewed industry guidance, such as the Institute of Internal Auditors' June 2010 publication, entitled *Global Technology Audit Guide (GTAG®) 14, Auditing User-developed Applications*; analysis and recommended best practices developed by a recognized IT research and advisory company; and NIST Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, dated October 2008; for information about risks and controls related to business-unit led application development.

- Observed interdivisional meetings held to develop policy and guidance associated with business unit-led application development to obtain an understanding of potential risks and controls related to such development.

- Obtained and reviewed available information regarding the number of applications developed by DRR and RMS and the associated costs. The purpose of this procedure

[23] Pub. L. 97-255, codified to 31 U.S.C. § 3512.
[24] Section 306 of the Chief Financial Officers Act (Pub. L. 101-576, codified to 31 U.S.C. § 9106) requires government corporations, such as the FDIC, to submit annual management reports to the Congress that include a statement on internal accounting and administrative controls consistent with the Federal Managers' Financial Integrity Act. The statement is included in the FDIC's Annual Report, for which DIT's Assurance Statement serves as input.

was to obtain an understanding of the extent to which business units in these divisions engage in application development activities.

- Selected a non-statistical sample[25] of four applications developed by DRR and RMS operating in the production environment as of April 11, 2013 from a population of business-developed applications identified by DRR and RMS, which consisted of 7 DRR applications and 14 RMS applications.[26] Because DRR and RMS did not maintain official information systems inventories, we were unable to verify that the population provided to us was complete. We reviewed the four applications to obtain an understanding of the IT governance, application development practices, and controls employed by FDIC's business units to develop the applications. We did not assess whether the applications were adequately designed or whether development policies, procedures, and guidance had been properly implemented.

  We judgmentally selected the four applications based on whether they met one or more of the following criteria:

  - Received data from, or provided data to, a major application
  - Contained PII or other sensitive information
  - Supported more than 100 users
  - Involved a development time of two months or more
  - Used data owned by another FDIC division

For reference purposes, we also judgmentally selected one of six APEX applications developed by DIT for the business divisions in the years 2008 through 2013. We selected the application because it contained PII or other sensitive information and had more than one software version. The table below identifies the applications that we selected.

[25] The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

[26] This population is a subset of the total universe of 16 and 53 business-developed applications identified by DRR and RMS, respectively, at the time our audit sample was selected. The population included only those applications in the production environment developed using APEX or Microsoft Access/Structured Query Language Server, as we considered applications developed with these tools to potentially have higher risk. As of August 30, 2013, DRR informed us that, after further review, its universe of business-developed applications totaled 23 (as opposed to the 16 referenced above when our sample was taken).

Objectives, Scope, and Methodology

Table: Sampled Applications

Application Number	Developed By	Application Type	Application Description
1	DRR's BIS	APEX	Tracks the inventory and status of the marketing and management of ORE assets assigned to ORE contractors.
2	DRR's BPM	APEX	Tracks DRR employees, positions, and vacancies through the onboarding process.
3	RMS' BADS	APEX	Automates the forms used for performance management and recognition of all pre-commissioned examiners.
4	RMS' ROMIGs	Microsoft Access/ Structured Query Language Server	Captures RMS' quarterly analysis of insured depository institutions with assets greater than $10 billion.
5	DIT	APEX	Tracks the status of background investigations for employees and contractors.

Source: Listings of DRR- and RMS-developed applications provided by DRR and RMS personnel, respectively, and a listing of DIT-developed APEX applications provided by DIT personnel. We refer to each application sampled by number (versus application name) for security purposes.

For the applications selected, we interviewed DRR, RMS, and DIT development personnel (as applicable). We also obtained and reviewed available SDLC documentation maintained in various repositories, including shared folders, SharePoint sites, and StarTeam. In general, this documentation related to application development activities that occurred during the period April 2010 through May 2013. We performed these audit procedures to determine whether DRR and RMS had established, through written policies, procedures, and guidance, controls designed to mitigate the key risks we identified related to business unit-led application development.

We performed our audit work at the FDIC's offices in Dallas, Texas, and Arlington, Virginia.

Internal Control, Reliance on Computer-processed Information, Performance Measurement, and Compliance with Laws and Regulations

As described in the Scope and Methodology section of this Appendix, we performed audit procedures to identify and obtain an understanding of the FDIC's established internal controls related to business unit-led application development activities. However, consistent with our audit objectives, we did not assess the implementation or effectiveness of those controls or the adequacy of the FDIC's overall internal control or management control environment. Our report identifies certain internal control gaps warranting management's attention.

Objectives, Scope, and Methodology

We did not rely on automated information from the FDIC's information systems that were significant to our audit objectives, conclusions, or findings. Accordingly, we did not assess the effectiveness of information system controls.

The Government Performance and Results Act of 1993 (the Results Act), as amended, directs Executive Branch agencies to develop a customer-focused strategic plan, align agency programs and activities with concrete missions and goals, and prepare and report on annual performance plans. We did not assess the strengths and weaknesses of the FDIC's annual performance plans in meeting the requirements of the Results Act because such an assessment was not significant to the audit objectives.

Regarding compliance with laws and regulations, our report identifies gaps in controls that, if not addressed, could result in non-compliance with federal statutes, such as the E-Government Act of 2002—particularly Section 208 regarding privacy impact assessments and title III (also known as FISMA) regarding information security. In addition, we assessed the risk of fraud and abuse related to our objectives in the course of evaluating audit evidence.

Glossary of Terms

Term	Definition
Application	Per FDIC Circular 1360.18, *FDIC Software Quality Assurance Policy*, the aggregate of information technology that processes, stores, and/or transmits information to satisfy client requirements, such as the need to inventory and track the marketing and management of assets.
Application Security Assessment (ASA)	An examination of the sensitivity level of the information processed by an application to determine the application's security category. This security category indicates the potential impact on the FDIC's mission if the confidentiality, integrity, and/or availability of the system and its data were compromised.
Assurance Statement	As part of the process for preparing the FDIC's Annual Report (see 31 U.S.C. § 3516(b)), division and office directors provide assurance to the FDIC Chairman after considering their division's or office's overall activities in conjunction with the results of management's on-going evaluations of internal control operations, programs, and systems along with the results of audits and reviews conducted by the FDIC OIG, GAO, or external firms. The assurance is communicated in the form of an assurance statement that addresses compliance with applicable internal control standards.
Business Unit-Led Application Development	The creation or enhancement of IT solutions where the development is performed under the direction of an FDIC business unit.
Configuration Management	The technical and administrative process to identify, document, and maintain configuration item integrity, control configuration item changes, and record and report on configuration item change processing status. A configuration item is a unit or aggregate of documentation, software and/or hardware that is designated for configuration management.
Enterprise Architecture	Describes the current and desired future state of the Corporation in terms of performance, business, data, services, technology, and security, and lays out a plan for transitioning from the current state to the desired future state. It captures and clarifies how various business processes, information system components, and people work together to accomplish the mission of the Corporation.
Federal Information Security Management Act (FISMA)	The Federal Information Security Management Act of 2002 (title III, E-Government Act of 2002), Pub. L. No. 107-347, dated December 17, 2002, requires federal agencies, including the FDIC, to develop, document, and implement an agency-wide information security program that provides security for the information and systems that support the operations and assets of the agency. In addition, FISMA requires agencies to perform annual independent evaluations of their information security programs and practices.

Glossary of Terms

General Support System (GSS)	An interconnected set of information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people.
Information Security Manager (ISM)	There are 12 ISMs throughout the FDIC, representing the FDIC divisions and offices. The DIT ISMs support DIT as well as the FDIC's executive offices. ISMs assess the level of security in information systems, determine which are major applications, ensure that security requirements are addressed, and promote compliance with FDIC security policies and procedures.
Information Technology (IT) Governance	The leadership, organizational structures and processes that ensure IT supports the FDIC's strategies and objectives.
Least Privilege	The practice of restricting user access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform a user's job.
Major Application	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss or misuse of, or unauthorized access to, or modification of the information in the application.
Minor Application	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Such applications are typically part of a GSS or major application.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the Department of Commerce's Technology Administration. As part of its responsibilities, NIST develops and publishes technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive, but unclassified, information in federal computer systems.
Oracle® Application Express (APEX)	A web browser-based rapid application development tool provided as part of the Oracle® Database software.
Personally Identifiable Information (PII)	Any information maintained by an agency about an individual, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, etc., including any other personal information that is linked or linkable to an individual. The definition of PII is similar in meaning to the definition of the term "information in identifiable form," as used in the E-Government Act of 2002.

Glossary of Terms

Privacy Impact Assessment (PIA)	A process for (1) examining the risks and ramifications of using information technology to collect, maintain, and disseminate PII from or about members of the public and (2) identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. The requirement for PIAs flows from Section 208 of the E-Government Act of 2002, which states that agencies (including the FDIC) are required to conduct—prior to developing or acquiring information technology containing PII—an assessment of the agencies' use of such PII by the technology at issue.
Privacy Threshold Analysis (PTA)	A preliminary analysis to determine whether a PIA, or any other privacy compliance documents, is required.
Production Environment	The end-user environment containing the current version of an application that has successfully passed testing and has received approval for promotion into the environment.
Rational Unified Process® (RUP®)	A comprehensive process framework that provides industry-tested practices for software and systems delivery and implementation and for effective project management. RUP® is the standard systems development life cycle methodology used by DIT for the information technology projects it manages. Currently, only DIT is required to use this standard.
Regional Office Management Information Groups (ROMIGs)	Created in 1996 to fulfill management information and automation needs in the operations of each RMS regional office, ROMIGs provide senior regional management with a highly specialized and flexible resource to meet RMS information demands.
Risk Management	The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level in order to protect information resources.
Section 508	Section 508 of the Rehabilitation Act (Pub. L. 93-112, as added Pub. L. 99-506, and codified to 29 U.S.C. § 794d) requires, in general, that agencies ensure that information technology that they develop or acquire be as accessible to persons with disabilities as it is to persons without disabilities.
Security Category	FISMA requires federal agencies to categorize their information assets in accordance with NIST standards. NIST Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, which the FDIC has adopted as policy, sets forth standards for categorizing federal information and information systems based on the FISMA objectives of providing appropriate levels of information security according to a range of risk levels. The publication defines three levels of potential impact (i.e., High, Moderate, and Low) that could occur should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The FDIC's approach for assigning impact-level ratings is defined in

Glossary of Terms

	Circular 1360.8, *Information Security Categorization*. Categorizing information and information systems is a critical first step in establishing appropriate security because the categorization is used to determine the minimum set of baseline security controls required to protect the information and information systems.
Sensitive Information	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. Such information includes PII; confidential financial information from third parties; as well as information about insurance assessments, resolution and receivership activities, and enforcement, legal, and contracting activities.
Separation of Duties	Addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. In the context of information technology, separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.
Systems Development Life Cycle (SDLC)	The phases included in the life of an information system. A typical SDLC includes five phases: initiation, development/acquisition, implementation/assessment, operations/maintenance, and disposal. Each phase involves specific tasks and work products and may be repeated over the life of the information system.
Work Products	Work products, as that term is used in this report, refers to SDLC documents, such as IT project proposals, checklists, ASAs, PTAs, testing plans and summaries, etc.

Acronyms and Abbreviations

Acronym or Abbreviation	Explanation
APEX	Application Express
BADS	Business Analysis and Decision Support
BIS	Business Information Systems
BPM	Business Program Management
CIO	Chief Information Officer
CIRC	Capital Investment Review Committee
DIT	Division of Information Technology
DOA	Division of Administration
DRR	Division of Resolutions and Receiverships
DSC	Division of Supervision and Consumer Protection
EA	Enterprise Architecture
EA-Rep	Enterprise Architecture Repository
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PRC	RMS IT Portfolio Review Committee
Pub. L.	Public Law
RMS	Division of Risk Management Supervision
ROMIGs	Regional Office Management Information Groups
RUP®	Rational Unified Process®
SDLC	Systems Development Life Cycle
SGB	DRR Systems Governance Board
U.S.C.	United States Code

Corporation Comments

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

DATE: September 6, 2013

TO: Stephen M. Beard
Deputy Inspector General for Audits and Evaluations

FROM: Martin D. Henning /**Signed**/
Acting Chief Information Officer

SUBJECT: Management Response to the Draft Evaluation Report Entitled, *The FDIC's Controls Over Business Unit-Led Application Development Activities* (Assignment No. 2013-018)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) August 2, 2013 draft report on FDIC's controls over business unit-led application development. In its report, the OIG made three recommendations to the Chief Information Officer (CIO). Based on the overall results of the audit, the CIO agrees that additional steps should be taken to enhance the controls supporting the FDIC's business unit-led application development activities.

Specifically, we agree that all FDIC applications should be recorded in a corporate database, that the start of application development should be better governed, that application deployment should be better governed, and that the costs of development should be better managed. We agree that a flexible system development lifecycle standard should be used to achieve these objectives. Finally, we agree that a review of existing applications developed outside of DIT should be completed to ensure they comply with FDIC security policies.

We carefully considered and concur with each of the recommendations made by the audit team. Corrective actions for each recommendation are planned or in process. Our specific responses for each of the recommendations are provided below.

Corporation Comments

Management Response

Recommendation 1, Information Systems Inventory and IT Governance
Recommend that the Acting CIO include language in the planned corporate policy on business unit-led application development that requires FDIC business units to:

a) coordinate with DIT to ensure that applications developed by business units are recorded in the Corporation's information systems inventory, when appropriate; and

b) develop written IT governance processes that address the review and approval of development proposals, the decision making-process for authorizing the deployment of applications to the production environment, and the tracking and reporting of application development costs.

Management Decision:
1(a) Concur - The planned corporate policy will require FDIC business units to coordinate with DIT to ensure that applications developed by business units are recorded in the Corporation's information systems inventory, when appropriate;

1(b) Concur and propose alternate action - The planned corporate policy would require the application of existing written IT governance processes at levels appropriate for the size, complexity, and sensitivity of the subject application. It would also provide direction on the use of FDIC financial systems to track and report on application development costs.

Corrective Action Plan with Dates:
The corporate policy on business unit-led application development is being drafted and will be submitted to the Division of Administration (DOA) by October 1, 2013.

We plan for the draft corporate policy to be finalized and published by January 31, 2014. DOA will post the draft corporate policy for the standard 10 business days and collect feedback from employees. DIT will review the feedback, make responsive changes to the policy where possible, and identify where changes were not possible with reasons before publishing the final directive. Because of the expectation that this draft policy will receive significant employee feedback, we believe several weeks are required to read the feedback and make responsive changes collaboratively with the divisions affected. Following our final changes, a review and approval process by organizations such as Legal and DOA's Human Resources Branch is required. After addressing comments from these organizations, the final directive will be published.

Recommendation 2, System Development Life Cycle Standards
Recommend that the Acting CIO coordinate with FDIC business units involved in application development to establish appropriate written SDLC standards that are consistent with applicable laws, policies, and guidelines, and commensurate with the risks and complexity of their development activities.

Corporation Comments

Management Decision: Concur

Corrective Action Plan with Date:
The planned corporate policy will direct business units developing applications and DIT's Project Management Office to work together to apply the existing FDIC SDLC commensurate with the risks and complexity of new development activities. This collaboration will begin immediately and be formalized with the implementation of the corporate policy no later than January 31, 2014.

Recommendation 3, Information Security and Privacy
Recommend that the Acting CIO coordinate with DRR and RMS to ensure that existing applications developed under the divisions' direction comply with FDIC security policies pertaining to sensitivity assessments, privacy reviews, security plans, access control reviews, and separation of duties.

Management Decision: Concur

Corrective Action Plan with Dates:
DIT will coordinate with DRR and RMS to record all business-developed applications DRR and RMS identify in the Corporation's information systems inventory (Enterprise Architecture Repository). This activity will be completed October 15, 2013.

DIT will review DRR and RMS identified business-developed applications for non-compliance with FDIC security policies pertaining to sensitivity assessments, privacy reviews, security plans, access control reviews, and separation of duties. If an application is found to be noncompliant with FDIC security policies, non-compliance issues will be cataloged and communicated to the divisions. Remedial actions necessary will be identified in the review and will have specific owners and due dates commensurate with the severity of the flaw(s) identified. This review will be completed April 15, 2014.

Any questions regarding this response should be directed to Rack Campbell at (703) 516-1422.

cc: Bret D. Edwards, Director, Division of Resolutions and Receiverships
Doreen R. Eberley, Director, Division of Risk Management Supervision
Russell G. Pittman, Director DIT
James H. Angel, Jr., Deputy Director, DOF, Corporate Management Control
Christopher J. Farrow, Acting CISO, Information Security & Privacy
John S. Kidd, Acting Deputy Director, DIT, Infrastructure Services Branch
David K. Lanphear, Acting Director, DIT, Enterprise Technology Branch
Steven P. Anderson, Deputy Director, DIT, Business Administration Branch
Kaj D. Vetter, DIT Chief, Program Management Office
Rack D. Campbell, DIT Chief, Audit and Internal Control

3

Summary of the Corporation's Corrective Actions

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1.	The FDIC will issue a corporate policy on business unit-led application development that requires the FDIC's business units to coordinate with DIT to ensure that applications developed by business units are recorded in the Corporation's information systems inventory, when appropriate. The policy will also require the application of existing written IT governance processes at levels appropriate for the size, complexity, and sensitivity of applications and provide direction for tracking and reporting application development costs.	January 31, 2014	N/A	Yes	Open
2.	The planned corporate policy on business unit-led application development will direct the FDIC's business units developing applications and DIT's Project Management Office to work together to apply the FDIC's existing SDLC commensurate with the risks and complexities of new development activities.	January 31, 2014	N/A	Yes	Open
3.	DIT will coordinate with DRR and RMS to record business-developed applications in the Corporation's information systems inventory, as appropriate. DIT will review DRR and RMS identified business-developed applications for non-compliance with FDIC security policies. If instances of non-compliance are identified, such instances will be catalogued and communicated to the appropriate division(s). Any remedial actions will be assigned to an owner and milestones will be established	April 15, 2014	N/A	Yes	Open

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]
	commensurate with the severity of the non-compliance.				

[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 (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.