Office of Inspector General

September 2005
Report No. 05-037

Controls Over the Risk-Related Premium System

AUDIT REPORT

Office of Audits

Background and Purpose of Audit

The Risk-Related Premium System (RRPS) is the FDIC's system of record for the risk assessment classification of financial institutions. The RRPS contains examination and supervisory action information that is considered highly sensitive and is not available to the public. The insurance premium assessed to each institution is based on the balance of insured deposits held during the preceding two quarters and on the degree of risk the institution poses to the Bank Insurance Fund or the Savings Association Insurance Fund. The FDIC uses a risk-based premium system that assesses higher rates on those institutions that pose greater risks to the insurance fund.

The RRPS calculates assessment rates based on data from such sources as the institutions' Call Reports; Thrift Financial Reports; examination data from the FDIC, Office of the Comptroller of the Currency, Federal Reserve Board, and Office of Thrift Supervision; and input from FDIC personnel.

The audit objective was to determine whether the RRPS application provides the appropriate level of confidentiality, data integrity, and availability through the use of effective management, operational, and technical controls.

To view the full report, go to www.fdicig.gov/2005reports.asp

Report No. 05-037
September 2005

Controls Over the Risk-Related Premium System

Results of Audit

We concluded that the management, operational, and technical controls for the RRPS provide reasonable assurance of adequate security. The confidentiality, integrity, and availability of the system and associated data were maintained through a combination of sound controls including:

- risk assessments and security reviews,
- logical access controls,
- data integrity edit checks, and
- business continuity planning.

In addition, the FDIC has developed a certification and accreditation (C&A) process to validate that the security controls implemented in an information system are commensurate with risks throughout the FDIC's computing environment. In August 2005, the FDIC started the C&A for the RRPS, which includes extensive testing of the key management, operational, and technical controls.

Although key application controls generally operated as intended, we identified the following deficiencies:

- the RRPS security plan did not fully and accurately describe the current management, operational, and technical controls;
- a software configuration management (SCM) plan was not fully developed or implemented; and
- read and write access rights of RRPS users were not periodically reviewed.

These deficiencies posed the following risks to the RRPS:

- not all appropriate security controls for RRPS have been considered and implemented,
- improper and/or unauthorized software changes could be made to RRPS, and
- RRPS data could be changed or improperly disclosed by individuals who no longer need RRPS read and write capabilities.

Collectively, these deficiencies pose risks to the confidentiality, integrity, and availability of the RRPS; however, the risks are at least partially mitigated by the ongoing C&A process.

Recommendations

We recommended that the FDIC:

- correct identified deficiencies in and approve the updated RRPS security plan,
- develop and implement an SCM plan for RRPS, and
- conduct semiannual reviews of all RRPS user access rights.

FDIC management agreed with the recommendations and has taken actions to address them.

TABLE OF CONTENTS

Federal Deposit Insurance Corporation
801 17th Street NW, Washington, DC 20434

Office of Audits
Office of Inspector General

DATE: September 23, 2005

MEMORANDUM TO: Arthur J. Murton, Director
Division of Insurance and Research

Michael E. Bartell
Chief Information Officer and
Director, Division of Information Technology

FROM: Russell A. Rau [Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: *Controls Over the Risk-Related Premium System*
(Report No. 05-037)

This report presents the results of the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) audit of system controls over the Risk-Related Premium System (RRPS). The RRPS, a major application,[1] is the FDIC's system of record for the risk assessment classification of financial institutions and is housed in the FDIC's Virtual Supervisory Information on the Net (ViSION) Application.[2] The RRPS contains examination and supervisory action information that is considered highly sensitive and is not available to the public. The objective of this audit was to determine whether the RRPS application provides the appropriate level of confidentiality, integrity, and availability through the use of effective management, operational, and technical controls. Appendix I describes in detail our objective, scope, and methodology.

BACKGROUND

The FDIC maintains the Bank Insurance Fund (BIF) and the Savings Association Insurance Fund (SAIF) by assessing depository institutions an insurance premium twice a year. The premium amount is based on the balance of assessable deposits held during the preceding two quarters and on the degree of risk the institution poses to the insurance fund. The FDIC's risk-based premium system assesses higher rates for institutions that pose greater risks to the BIF or SAIF. To assess premiums, the FDIC places each institution in one of nine risk categories using a two-step process based first on capital ratios and second on other relevant information such as the results of:

- the last examination by the primary federal regulator;

[1] OMB Circular A-130, Appendix III, defines a major application as one that requires special 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. The FDIC has designated seven applications, including the RRPS, as major applications.

[2] ViSION is an FDIC major application and mission-critical system that provides access to financial, examination, and supervisory information on financial institutions.

- independent, joint,[3] or concurrent FDIC examinations; and
- off-site statistical analysis of reported financial statements.

The RRPS calculates assessment rates based on data from such sources as Call Reports; Thrift Financial Reports; examination data from the FDIC, Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), and Office of Thrift Supervision (OTS); and input from FDIC personnel. In accordance with guidelines approved by the FDIC Board of Directors, the Division of Insurance and Research (DIR) uses this information to determine the assessment rate for each institution. Appendix II contains an overview of the RRPS.

DIR performs the assessment process twice a year. During this process, DIR assigns and updates the assessment risk classifications for all financial institutions. The financial institutions receive quarterly assessments based on the assessment ratings. At the completion of each assessment period, DIR meets with the Division of Information Technology (DIT) to discuss RRPS changes that may be needed as a result of possible revised legislative requirements or new system capabilities. When system changes are made, the RRPS is retested prior to the next assessment period. DIR is responsible for the RRPS; however, the Division of Supervision and Consumer Protection (DSC) has the majority of RRPS users (about 2,000).

Application Control Guidance

The Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, requires each federal agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. Under FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for federal agency operations and assets. NIST issued Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* which states that security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, taken together, should adequately protect the confidentiality, integrity, and availability of the system and its information. SP 800-53 defines these security controls as follows.

- **Management controls** focus on the management of risk and the management of information system security. These controls address: (1) risk assessment; (2) security planning; (3) acquisition of information systems and services; and (4) certification, accreditation, and security assessments.

- **Operational controls** are primarily implemented and executed by people (as opposed to systems). These controls address: (1) personnel security, (2) physical and environmental protection, (3) contingency planning and operations, (4) configuration management, (5) hardware and software maintenance, (6) system and information integrity, (7) media protection, (8) incident response, and (9) security awareness and training.

[3] An examination performed by both the FDIC and another federal or state regulatory agency.

- **Technical controls** are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware[4] components of the system. These controls address: (1) user identification and authentication, (2) logical access control, (3) audit and accountability, and (4) system and communications protection.

System Certification and Accreditation (C&A)

NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, states that agency officials must have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions regarding whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation are developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision. The steps performed in the C&A process are dependent on the level of risk defined as low-, moderate-, or high-impact in an operating system.

The FDIC has developed a C&A process to validate that the security controls implemented in an information system are commensurate with the risks throughout the FDIC computing environment. In July 2004, the FDIC performed a low-impact C&A for the RRPS which, according to NIST guidance, entails only a documentation review of the controls. Beginning in 2005, the FDIC planned to perform a moderate-impact C&A, which includes extensive testing of key management, operational, and technical controls, for all of its major systems, including the RRPS. The C&A for the RRPS began in August and will be completed by December 2005.

RESULTS OF AUDIT

The management, operational, and technical controls for RRPS provide reasonable assurance of adequate security. The confidentiality, integrity, and availability of the system and associated data were maintained through a combination of sound controls, including:

- risk assessments and security reviews,
- logical access,
- data integrity edit checks (details are provided in Appendix III), and
- business continuity planning.

[4] Firmware is hardware that includes embedded software, i.e., a read-only or programmable read-only memory chip.

Although key application controls generally operated as intended, we identified the following deficiencies in the security plan, software configuration management, and access reviews that could affect the security of the RRPS.

.

- The security plan did not fully and accurately describe the current management, operational, and technical controls (Finding A).
- A software configuration management (SCM) plan was not fully developed or implemented (Finding B).
- RRPS users' read and edit access rights were not periodically reviewed (Finding C).

As a result of these deficiencies, the RRPS is exposed to the following risks:

- Not all appropriate security controls for RRPS have been considered and implemented.
- Improper and/or unauthorized software changes could be made to RRPS.
- RRPS data could be changed or improperly disclosed by individuals who no longer need read and edit capabilities.

Collectively, these deficiencies pose risks to the confidentiality, integrity, and availability of the RRPS; however, the risks are at least partially mitigated by the ongoing C&A process.

FINDINGS AND RECOMMENDATIONS

FINDING A: SECURITY PLAN

Condition: The RRPS security plan, dated March 29, 2005, adequately addressed the RRPS system security controls. However, some of the plan's elements need to be more fully explained. The results of our assessment of the RRPS security plan based on NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, are summarized in Table 1.

Table 1: Coverage of Elements in the RRPS Security Plan

Security Plan Section	NIST SP 800-18 Requirements	Exceptions
System Identification	System Name/Title, Information Contacts, Assignment of Security Responsibility, System Operational Status, General Description/Purpose, System Environment, System Interconnection/Information Sharing, Applicable Laws or Regulations Affecting the System, General Description of Information Sensitivity	None
Management Controls	Risk Assessment and Management	The plan does not provide information on where and how to obtain the most recent Risk Assessment Report.
	Review of Security Controls	None
	Rules of Behavior	The plan does not specify a requirement to provide users with a copy of the Rules of Behavior prior to obtaining access to RRPS.
	Planning for Security in the Life Cycle	The plan does not describe disposal requirements for system termination such as procedures on how information would be archived, cleared, or purged from the RRPS.
	Authorize Processing	None
Operational Controls	Personnel Security	The plan does not indicate the sensitivity level (low, medium, and high) designations for DIT contractor personnel involved in RRPS maintenance and technical support. The plan does not specify termination procedures for users in adverse situations. Note: FDIC Circular 1360.15, *Access Control for Automated Information Systems*, is referenced as containing procedures for reviewing user access. The reviews have not been performed (see Finding C).
	Physical and Environmental Protection	None
	Production, Input/Output Controls	Although the plan indicates that specific electronic processing procedures have been established to

Security Plan Section	NIST SP 800-18 Requirements	Exceptions
		handle data and media from external agencies, no information is included on where and how to obtain these procedures. Labeling the data sensitivity (e.g., Privacy Act or proprietary data) of printed output is not addressed.
	Contingency Planning	None
	Application Software Maintenance Controls	The plan does not require that a Configuration Management Plan be developed and implemented as required by FDIC Circular 1320.4, *FDIC Software Configuration Management Policy* (see Finding B). The plan does not address migration procedures (i.e., movement of the software through the development stage to the test stage to the production stage) to prevent using incorrect versions of software.
	Data Integrity/Validation Controls	None
	Documentation	None
	Security Awareness and Training	None
Technical Controls	Identification and Authentication	None
	Logical Access Controls	None
	Public Access Controls	None
	Audit Trails	None

During our fieldwork, we provided DIR with the security plan exceptions noted in this report. The ISM, in coordination with DIT personnel, immediately began addressing our concerns.

Cause: The deficiencies noted in the RRPS security plan were similar to those identified in a previous Independent Security Review conducted in 2003. The DIR Information Security Manager (ISM) responsible for RRPS did not verify and ensure that all of the previously identified deficiencies had been corrected before the March 29, 2005 security plan was approved.

Criteria: A security plan for an information system helps to ensure that agreed-upon security controls planned or in place are fully documented. In addition, the security plan provides a complete description of the information system, including supporting documentation such as the key documents that support an organization's information security program. Office of Management and Budget (OMB) Circular A-130, Appendix III, requires that agencies prepare security plans for their general support systems and major applications. OMB outlines the minimum controls that must be described in system and application security plans and requires that security plans comply with NIST standards.

NIST SP 800-18 states that the purposes of system security plans are (1) to provide an overview of the security requirements of the system and description of the controls in place or planned that meet those requirements and (2) to delineate the responsibilities and expected behavior of all individuals who access the system.

NIST SP 800-53, control number PL-1, *Security Planning Policy and Procedures*, states that the organization develops, disseminates, and periodically reviews/updates: (1) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (2) formal documented procedures to facilitate the implementation of the security planning policy and associated security planning controls. Further, SP 800-53, control number PL-3, *System Security Plan Update*, states that the organization should review the security plan for the information system to address system/organizational changes or problems identified during the plan implementation or security control assessments.

NIST SP 800-37 states that security plans should be updated and approved prior to the assessment of security controls during the C&A process.

FDIC Circular 1310.3, *Information Technology Security Risk Management Program*, dated July 6, 2005, states that the divisional program manager is responsible for preparing a security plan that documents the management, operational, and technical security controls intended to protect information assets. The circular incorporates guidance included in NIST publications.

Effect: The RRPS security plan does not fully address the requirements described in NIST SP 800-18. Therefore, there is a risk that not all appropriate security controls for RRPS have been considered and implemented to protect the confidentiality, integrity, and availability of the system and the data it processes. The deficiencies we identified in the security plan could result in the following:

- The most current risk assessment may not be used to mitigate security risks if there is no reference to the location and date of the latest risk assessment performed. Consequently, the wrong set of risks could be mitigated, or the high risks may not be addressed.
- New users may not be aware of their security responsibilities when accessing RRPS if they are not provided with the Rules of Behavior prior to receiving system access. User awareness training, which includes the Rules of Behavior, is given only once a year.
- Sensitive information in RRPS could be exposed to unauthorized access at the end of the system life cycle if disposal requirements are not defined and planned.
- Risk of unauthorized activities could increase if the appropriate level of screening of the contractor personnel involved in system maintenance and technical support is not performed because position sensitivity levels (low, medium, and high) have not been designated.
- Risk of unauthorized activities of disgruntled employees could increase if termination procedures for users under adverse situations are not readily identified and available.
- Risk of improper disclosure of sensitive data could increase if procedures for handling the receipt of sensitive data and media from external agencies are not readily identified and available.

- Risk of unauthorized disclosure of sensitive information (e.g., Privacy Act or proprietary data) could increase if there is no requirement to properly label the sensitivity level of printed output data.
- Risk of errors and omissions from incorrect versions of software placed into production could increase if formal migration procedures (development to test to production procedures) are not readily identified and available.

The risks posed by the deficiencies in the security plan are heightened because of the changing control environment affecting RRPS. As a result of the FDIC's reorganization and transformation, key RRPS personnel have departed, and the status of the remaining personnel and contractors is uncertain. Keeping policies, procedures, and system documentation as current and complete as possible is critical in ensuring the adequacy of controls for system operations in a changing environment.

RECOMMENDATION

(1) We recommend that the Director, DIR, correct the deficiencies in and approve the updated RRPS security plan.

CORPORATION COMMENTS AND OIG EVALUATION

On September 13, 2005, the Director, DIR, provided a written response that is presented in its entirety in Appendix V of this report. DIR agreed with the recommendation and provided a copy of the revised security plan. The revised security plan adequately addressed the deficiencies summarized in Table 1 of this report. DIR also indicated that the security plan will be modified when: (1) NIST or OMB update requirements for major application security plans, (2) RRPS application controls or procedures are modified, and/or (3) internal reviews or external security audits require modifications. The security plan is expected to be approved by October 14, 2005.

The actions taken and planned by management are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

FINDING B: SOFTWARE CONFIGURATION MANAGEMENT

Condition: The RRPS project team did not develop an SCM plan in accordance with FDIC and NIST guidelines. Specifically, the RRPS Project Team did not develop an SCM plan in accordance with the FDIC's SCM plan guidance.

The March 29, 2005 RRPS security plan referenced the RRPS *Maintenance Manual*, dated November 2002, as the source for maintaining and updating software configuration. The *Maintenance Manual* contains project documentation references, points of contact, system description, and the process for handling change requests. However, as indicated in Table 2 on the next page, the *Maintenance Manual* does not adequately address required plan elements

specified in FDIC guidelines. Appendix IV provides a detailed description of the SCM plan elements as described in the FDIC's *Software Configuration Management Guidebook*, dated July 22, 2003.

Table 2: SCM Plan Elements Not Addressed in the RRPS *Maintenance Manual*

SCM Plan Element	Plan Requirements
CM Organization	Roles and Responsibilities (Includes only names of contacts)
	Tools/Environment
	Training
Configuration Identification	Identification Methods
Configuration and Change Control	CM Repository
	View and Branch Management
	Project Baselines
	Document Processing and Approval
	Change Request Processing and Approval (Focus was on the form of the request)
	Change Control Board
	Release Process
Status Accounting	Reports
Configuration Evaluations	Physical Configuration Audit
	Functional Configuration Audit
	Milestones
	Subcontractor and Vendor Software Control

The RRPS Project Team is using two SCM tools in the absence of a formal SCM plan--StarTeam for the software residing on the servers and Endevor for the software residing on the mainframe.[5] However, only two StarTeam capabilities had been implemented at the time of our review--software documentation and a change request facility. The following key StarTeam capabilities have not been implemented:

- software release comparison with date/time stamp;
- change tracking and traceability;
- file locking to prevent simultaneous access between users;
- workflow control for approval process; and
- rollback to previous software version.

Key features of Endevor have been implemented to control changes and access to the RRPS software residing on the mainframe.

[5] RRPS is considered a client/server application. The functions of client/server applications are distributed between different computer platforms such as servers and the mainframe.

Cause: The RRPS Project Team indicated that factors such as the recent DIT reorganization and contract consolidation efforts affected the completion of the SCM plan for RRPS. As a result, work on both the SCM plan and StarTeam implementation was delayed until June 2005.

Criteria: An SCM program ensures that the integrity of the system software is maintained during a system's life cycle. Key components of an SCM program include developing an SCM plan and using automated tools to track and control software changes.

NIST SP 800-53, CM-2, *Baseline Configuration,* calls for organizations to develop, document, and maintain a current baseline configuration of an information system and an inventory of the system's constituent components. CM-2 also indicates that an organization should update the baseline configuration as an integral part of information system component installations and should employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration. CM-3, *Configuration Change Control,* states that an organization should document and control changes to an information system. Information system changes should be approved by appropriate organizational officials in accordance with organizational policies and procedures.

FDIC Circular 1320.4, *FDIC Software Configuration Management Policy,* dated July 8, 2003, states that an SCM plan should be developed and implemented for all applications no later than December 31, 2003. The circular includes specific responsibilities and guidance for preparing and implementing the plan. The system development representative (project manager) is responsible for preparing the SCM plan. The circular requires that application SCM plans and SCM tools comply with the procedures described in the *Software Configuration Management Guidebook*, dated July 22, 2003.

Effect: DIT recently completed an organizational transformation that resulted in consolidating the number of application support contractors. The current RRPS contractor was not named as one of the four remaining contractors. As a result, the current contractor may not be supporting RRPS in the future. In addition, DIT has downsized and has lost many personnel, including an FDIC RRPS project manager. To facilitate the reassignment of responsibilities, current and explicit RRPS software configuration management processes must be in place to ensure that system documentation and SCM procedures are understood by new FDIC or contractor personnel.

Without an SCM plan, the RRPS could be exposed to unauthorized changes, errors, and omissions that could damage critical data and cause system failures. More specifically, without implementing StarTeam, which contains key features needed for controlling software changes, the RRPS could experience the following:

- errors from changes made to the wrong versions of the software,
- an inability to trace change requests for problem resolution and/or verification that changes met requirements,
- an inability to prevent simultaneous updates to one file,
- errors from incorrect processing of approved changes, and
- an inability to revert to a previous software version in the event of a serious error.

RECOMMENDATION

(2) We recommend that the Director, DIT, develop and implement an SCM plan for RRPS that incorporates the appropriate features of StarTeam.

CORPORATION COMMENTS AND OIG EVALUATION

On September 18, 2005, the Director, DIT, provided a written response to the draft report that is presented in Appendix VI of this report. DIT agreed with the recommendation and stated that the SCM plan template was changed on July 29, 2005. DIT has drafted a new RRPS SCM plan using the updated template. In addition, four of the five StarTeam capabilities identified in the audit will be activated in StarTeam and included in the SCM plan for RRPS. A separate document addressing the workflow control for the approval process will be prepared.

The actions taken and planned by management are responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective actions have been completed and are effective.

FINDING C: ACCESS REVIEWS

Condition: The ISM responsible for RRPS reviewed access rights for 21 system administrators involved in the development and production of mainframe applications. However, the ISM did not periodically review the access rights for the majority of RRPS users. DSC has about 2,000 users, and at least 465 users had both read and edit capabilities. During the audit, we asked DSC Regional Managers to review their staffs' continued need for read and edit capabilities for the RPPS. The feedback we received from 5 DSC regional offices indicated that 75 of the 465 users no longer required the edit capability. The results indicated that 72 of the 75 users no longer needed access because of role changes and that 3 users were no longer employed at the FDIC. The access reviews by DSC Regional Managers are summarized in Table 3.

Table 3: Access Reviews by DSC Regional Managers

Region	Users with Read/Edit Access Rights	Users Who No Longer Need Read/Edit Access
Atlanta	82	2
Dallas	122	23
San Francisco	81	24
Kansas City	93	7
New York	87	19
Total	**465***	**75***

*The total does not include the Chicago Region because the requested information was not provided. We did not examine the need for the read-only capability in this audit.

Cause: DIR's ISM had not established the roles, responsibilities, and procedures for performing periodic access reviews of RRPS users as required by FDIC Circular 1360.15 and the RRPS security plan.

Criteria: User access to the RRPS should be granted based on the user's need to perform assigned duties and should be terminated when no longer required. NIST SP 800-53 states that

an effective information security program should include periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of an organization. Also, SP 800-53, PS-5, *Personnel Transfer,* states that an organization should review access authorizations when individuals are reassigned or transferred to other positions within the organization and should initiate appropriate actions such as closing old accounts, establishing new accounts, and changing system access authorization. SP 800-53, PS-4, *Personnel Termination,* states that an organization should terminate system access when employment is terminated.

FDIC Circular 1360.15, *Access Control for Automated Information Systems*, requires the ISM to review the assignment of user rights to sensitive information systems within his/her specific division or office. The RRPS security plan states that the ISM should review RRPS user access rights semiannually to determine whether users need them to perform their responsibilities.

Effect: Without periodic reviews of users' access rights, there is a risk that improper disclosure and/or unauthorized changes to RRPS data could be made by individuals no longer needing the read/edit capability. However, this access risk has been mitigated because: (1) DSC users' read and edit access is limited to the banks assigned to their respective Case Managers;[6] (2) Case Managers are required to manually record any changes that are made and to provide comments in the RRPS about the changes; and (3) after the caseload[7] is reconciled, the Case Managers send the hardcopy logs and management reports semiannually to the Assistant Regional Director for approval.

RECOMMENDATION

(3) We recommend that the Director, DIR, establish roles, responsibilities, and procedures for conducting periodic reviews of all RRPS user access rights as required by FDIC Circular 1360.15 and the RRPS security plan.

[6] A Case Manager performs activities related to the review, analysis, and processing of reports of examination, applications, investigations, and other correspondence involving their caseloads. The primary responsibilities of Case Managers involve assessing risk to the deposit insurance fund and directing the appropriate supervisory efforts to eliminate or manage such risk.

[7] A caseload may consist of organizations that have operations extending beyond the geographic boundaries of the region to which Case Managers are assigned. Regardless of geographic location, Case Managers will be the principal supervisory contact for the FDIC's regulatory oversight activities for the banking operations of institutions assigned to their caseloads.

CORPORATION COMMENTS AND OIG EVALUATION

DIR agreed with the recommendation and provided a copy of the procedures in the revised security plan. The revised security plan included the roles, responsibilities, and procedures for conducting periodic reviews of all RRPS user access rights. As stated earlier, the security plan is expected to be approved by October 14, 2005.

Management's planned action is responsive to the recommendation. The recommendation is resolved but will remain undispositioned and open until we have determined that agreed-to corrective action has been completed and is effective.

APPENDIX I

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine whether the RRPS application provided an appropriate level of confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

Scope

This audit is one of three audits being performed as part of an overall review of the RRPS process. The results of the other audits, *Audit of FDIC Assessments and Designated Reserve Ratio Determinations* (Assignment No. 2005-032) and *Audit of the FDIC's Risk-Related Insurance Premium System* (Assignment No. 2005-033), will be issued in separate reports. This audit covered the period from January 1, 2005 through June 30, 2005 and included the data upload for the financial institutions' December 31, 2004 Call Reports.

Methodology

To accomplish our objective, we determined whether the input, output, and processing controls minimized the risks of errors, omissions, and unauthorized access. Specifically, we:

- Obtained and reviewed documentation in support of the system development life cycle for RRPS.
- Obtained, through interviews and observation, an overview of the RRPS application and interfacing systems.
- Performed an analysis of RRPS user access accounts.
- Interviewed DSC, DIR, and DIT staff responsible for authorizing RRPS and ViSION access through the FDIC Intranet.
- Reviewed policies, procedures, and documentation relating to user access and account maintenance.
- Reviewed the FDIC's policies, procedures, and practices relating to application security training for RRPS.
- Reviewed SCM policies, procedures, and practices and interviewed DIT and contractor staff regarding the SCM tools and processes used by the RRPS system developers.
- Selected a random sample of 43 institutions and compared the RRPS assessment data that was modified during the July 2004 assessment period to the assessment data used by AIMS II[8] in order to determine the accuracy and completeness of the safety and soundness and capital group data used in computing quarterly assessments.
- Compared the institutional data provided by the FRB, OCC, and OTS for the July 2005 assessment period with the institutional data in the RRPS Universe database to determine the completeness of the external data input process.

[8] Assessments Invoicing Management System II (AIMS II) invoices financial institutions quarterly for insurance premiums assessed to maintain the BIF and SAIF.

- Reviewed RRPS security plan and supporting documentation.
- Reviewed the March 2005 user satisfaction survey of 52 respondents to determine whether RRPS was meeting user needs.

We performed audit work in DIR's Washington, D.C., office and DIT's Virginia Square office. We performed the audit from April through July 2005 in accordance with generally accepted government auditing standards.

Internal Controls

We performed an assessment of the RRPS internal controls, including the control environment, risk assessment, control activities, information and communications, and application monitoring. As discussed in the audit report, we identified control weaknesses. Most significantly, as a result of the FDIC's restructuring and transformation activities, key FDIC and contractor personnel have departed. This loss of continuity could have a negative impact on the control environment and control activities. Keeping policies, procedures, and system documentation as current and complete as possible is critical in ensuring the adequacy of controls for system operations in a changing environment.

Performance Measures

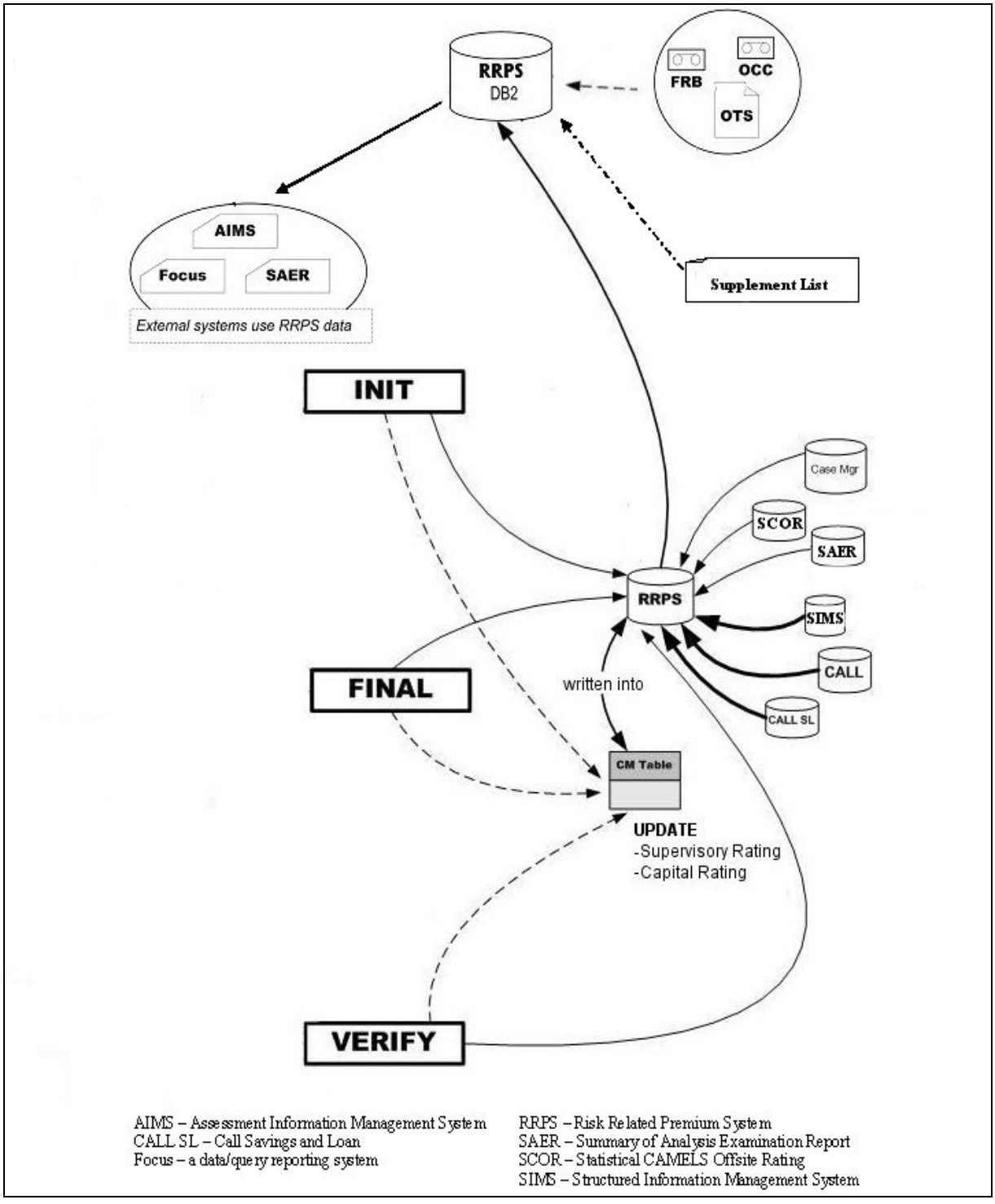
In relation to the FDIC's Insurance Program, the FDIC's *2005 Annual Performance Plan* states that the RRPS will be enhanced consistent with the improvements that are implemented for the ViSION application (which houses the RRPS). The RRPS has been enhanced and is undergoing additional enhancements consistent with the performance goal in the 2005 plan.

Reliance on Computer-based Data

As part of our audit objective, we assessed the reliability of the data in the RRPS system. Specifically, we compared the data in RRPS to the data received from external sources as part of the data integrity tests performed (see Appendix III). We did not compare system data to internal source data because that comparison was performed under another audit assignment. For purposes of this audit, the data was sufficiently reliable to support our audit conclusions.

APPENDIX II

RRPS SYSTEM OVERVIEW



APPENDIX III

DATA INTEGRITY TESTS*

Tests	Type of Test	Purpose	Method	Results
Ensure all records submitted by outside regulators are included in the Universe List.	Audit Command Language (ACL)	Completeness	Combined files from regulators into a file and compared the "CERT" column with the "CERT" column in the RRPS Universe List.	No issues. All records submitted by the regulators were included in the RRPS Universe List.
Locate the blank "RL [Reconcile-ment List] Codes" and determine why they are blank cells.	ACL	Completeness	Downloaded the Reconcilement List from RRPS. Used ACL to calculate the number of blank cells.	No issues. Found that 20 blank cells out of 572 total cells were identified. These discrepancies were resolved. Thirteen were manually deleted because they were "other insured branches" not institutions. Seven institutions were additions to the Reconcile-ment List because a recent examination may change the supervisory rating. The 20 "RL Code" cells were blank because the institutions were not originally listed on the Reconcilement List.
Ensure all records in the Reconcile-ment List are part of the Universe List.	ACL	Completeness	Filtered both lists to discard duplicate records. Compared the "CERT" field in both lists.	No issues. Found eight institutions on the Reconcilement List that were not on the Universe List. Institutions merged with other institutions.
Ensure that the internal logic of RRPS ensures an institution is assigned to the correct Capital Group (CG).	Code Review	Correctness of Calculation	Analyzed the logic of the latest version of the COBOL code in determining an institution's CG.	No issue. COBOL code would correctly perform the calculations to determine an institution's CG as required by DIR policy.
Ensure that the CG and Supervisory Subgroup (SS) determined by the RRPS were extracted by AIMS II.	Data Matching	Accuracy of RRPS data extracted by AIMS II to calculate institution assessments	Matched a statistical sample of 43 institutions to determine if the CG and SS generated by RRPS were used by AIMS II for invoicing.	The data from all 43 institutions were identical in RRPS and AIMS II.

* The accuracy of the data input into RRPS was not tested as part of the data integrity tests in this audit because (1) the other systems that RRPS obtains data from included built-in edit checks and (2) we are testing the accuracy of data input into RRPS by DSC personnel as part of a separate, ongoing audit.

APPENDIX IV

SCM PLAN ELEMENTS AS DESCRIBED IN THE *SOFTWARE CONFIGURATION MANAGEMENT GUIDEBOOK*

	Plan Requirement
CM* [configuration management] *Organization	
Roles and Responsibilities	Identify who is responsible for configuration management.
Tools/Environment	Identify the environment and software tools that will be used for configuration management throughout the application or product lifecycle.
Training	Describe the training required to implement the configuration tools and procedures.
Configuration Identification	
Identification Methods	Describe how configuration products are to be named, marked, and numbered. The identification scheme needs to cover hardware, system software, Commercial-Off-The-Shelf products, and all application development artifacts listed in the product directory structure such as plans, models, components, test software, results and data, executables, etc. Naming conventions for Endevor data sets should be described, if applicable.
Configuration and Change Control	
CM Repository	The FDIC has standardized the use of StarTeam and Endevor as the tools for managing the CM library. The CQMS [configuration and quality management staff] Team and the Infrastructure Services Branch are responsible for performing nightly backups, providing for disaster recovery and the general maintenance of the CM repositories. Describe any custom folders and discuss any custom security in place.
View and Branch Management	Describe the configuration to use multiple branches to segregate work, parallel development, introduction of code from external parties, or providing a gate between development and Development Integration.
Project Baselines	A baseline is a "snapshot" in time of one version of each artifact in the project repository. A baseline is the official standard on which subsequent work is based and to which authorized changes are made. The three main reasons for creating baselines are reproducibility, traceability, and reporting. Baselines also play a role in determining when an artifact needs to come under formal configuration and change control.
Document Processing and Approval	Documents that have a review level of either *Formal – External* or *Formal – Internal* require a review cycle and a documented review record.
Change Request Processing and Approval	The application will follow the Change Request processes and procedures in StarTeam. Describe any variation of the process by which problems and changes are submitted, reviewed, and dispositioned.
Change Control Board	Describes the membership and procedures for processing change requests.
Release Process	Describe what is in the release, who it is for, and whether there are any known problems, and installation instructions.

APPENDIX IV

Status Accounting	
Reports	Describe the content, format, and purpose of the requested reports and configuration audits. Reports are used to assess the "quality of the product" at any given time of the project or product life cycle. Reporting on defects based on change requests may provide some useful quality indicators and thereby alert management and developers to particularly critical areas of development.
Configuration Evaluations	Configuration evaluations are conducted to confirm that SCM activities and processes performed for an application are in compliance with FDIC standards and the resulting baselines and documentation are accurate.
Physical Configuration Audit	At the end of each iteration, the Project Manager or their representative will conduct a physical configuration audit to confirm that: • the change requests targeted for the iteration deployment are documented properly, • the artifacts changed against those CRs [change requests] are linked and that all appropriate artifacts are correctly labeled, • and the artifacts specified in the Development Case are either created, revised, or finalized. Describe any additional audits that will be conducted for the application. Reasons for doing so may involve regulatory requirements.
Functional Configuration Audit	Describes audit procedures to confirm that a baseline meets the requirements targeted for the baseline.
Milestones	Identify the internal and customer milestones related to the project or product CM effort. This section should include details on when the CM Plan itself is to be updated.
Subcontractor and Vendor Software Control	Describe how software from outside of application environment will be incorporated and reference any third party CM plans.

CORPORATION COMMENTS

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Division of Insurance and Research

September 13, 2005

TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits
Office of Inspector General

FROM: Arthur J. Murton [Electronically produced version; original signed by Arthur J. Murton]
Director

SUBJECT: Draft Report Entitled, *Audit of Controls Over the Risk-Related Premium System* (Assignment No. 2005-029)

Thank you for the opportunity to respond to the draft audit report, *Audit of Controls Over the Risk-Related Premium System*. The Division of Insurance and Research (DIR) agrees with the overall assessment that the management, operational, and technical controls for the Risk-Related Premium System (RRPS) provide reasonable assurance of adequate security.

The draft report contains three recommendations to maintain strong controls over RRPS. The Division is responsible for taking corrective action to address the deficiencies noted in the Recommendations One (1) and Three (3) of the draft report. The Division of Information Technology (DIT) is responsible for Recommendation Two (2) and will provide a response to the draft audit report under separate cover. The recommendations for which DIR has primary responsibility are listed below with the Division's responses and actions taken to correct noted deficiencies.

FDIC OIG Recommendations:

(1) We recommend that the Director, DIR, correct identified deficiencies in and approve the updated RRPS security plan.

DIR Response:

DIR concurs with the finding. All items listed in the condition have been documented in the RRPS security plan and a copy of the revised plan has been provided to the OIG. DIR will continue to modify the security plan when: (1) NIST/OMB updates requirements for major application security plans, (2) RRPS applications controls or procedures are modified, and/or (3) internal reviews or external security audits require modifications.

(2) We recommend that the Director, DIT, develop and implement an SCM plan for RRPS that incorporates the appropriate features of StarTeam.

DIT will respond to this finding under separate cover.

(3) We recommend that the Director, DIR, establish roles, responsibilities, and procedures for conducting periodic reviews of all RRPS user access rights as required by FDIC Directive 1360.15 and the RRPS security plan.

DIR Response:

DIR concurs with the finding. Roles, responsibilities, and procedures for conducting periodic reviews of all RRPS users access rights have been developed and are documented in the security plan.

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Division of Information Technology

DATE: SEP 16 2005

MEMORANDUM TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits

FROM: Michael E. Bartell
Chief Information Officer and
Director, Division of Information Technology
[Electronically produced version; original signed by Michael E. Bartell]

SUBJECT: Draft Report Entitled, *Audit of Controls Over the Risk-Related Premium System* (Assignment No. 2005-029)

Thank you for the opportunity to respond to the draft audit report, *Audit of Controls Over the Risk Related Premium System.* The Division of Technology (DIT) agrees with the overall assessment that the management, operational, and technical controls for the Risk-Related Premium System (RRPS) provide reasonable assurance of adequate security.

The draft report contains three recommendations to maintain strong controls over RRPS. The Division is responsible for taking corrective action to address the deficiencies noted in Recommendation Two (2) of the draft report. The Division of Insurance and Research (DIR) is responsible for Recommendations One (1) and Three (3) and will provide a response to the draft audit report under separate cover. The recommendation for which DIT has primary responsibility is listed below with the Division's response and corrective action.

FDIC OIG Recommendation:

(2) We recommend that the Director, DIT, develop and implement an SCM plan for RRPS that incorporates the appropriate features of StarTeam.

DIT Response:

The System Configuration Management Plan (SCMP) template was changed July 29, 2005 to reflect the implementation of the RUP SDLC implementation. A draft of the new RRPS SCMP was distributed for comments on August 30, 2005. The target date for completion of the RRPS SCMP is October 14, 2005. Four of the five StarTeam capabilities that the OIG determined to be missing at the time of the audit will be activated in StarTeam for RRPS and included as part of the new plan. Specifically, this includes: software release comparison with date/time stamp; change tracking and traceability; file locking to prevent simultaneous access between users; and rollback to previous software version. A second, separate document which addresses the fifth feature, workflow control for approval process, will also be completed by October 14, 2005.

cc: Jerry Russomano
Ron Pferchy
Nina Aggarwal
Al Gross
James H. Angel, Jr.
Arlinda G. Sothoron

APPENDIX VI

MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Dispositioned:[b] Yes or No	Open or Closed[c]
1	The security plan has been updated to correct the deficiencies identified during the audit. Approval of updated security plan is needed.	October 14, 2005	N/A	Yes	No	Open
2	The SCM Plan has been drafted, and the appropriate StarTeam capabilities will be implemented. Approval of the SCM Plan and StarTeam implementation is pending.	October 14, 2005	N/A	Yes	No	Open
3	The roles, responsibilities, and procedures for reviewing user access accounts are included in the updated security plan. Approval of the updated security plan is needed.	October 14, 2005	N/A	Yes	No	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(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] Dispositioned – The agreed-upon corrective action must be implemented, determined to be effective, and the actual amounts of monetary benefits achieved through implementation identified. The OIG is responsible for determining whether the documentation provided by management is adequate to disposition the recommendation.

[c] Once the OIG dispositions the recommendation, it can then be closed.