Office of Inspector General

December 13, 2001
Audit Report No. 01-025

Audit of the Least Cost Test Model

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20434
Office of Audits
Office of Inspector General

DATE: December 13, 2001

TO: Mitchell L. Glassman, Director
Division of Resolutions and Receiverships

Carol M. Heindel, Acting Director
Division of Information Resources Management and
Acting Chief Information Officer

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

SUBJECT: Report Entitled *Audit of the Least Cost Test Model*
(Audit Report Number 01-025)

The Office of Inspector General (OIG) completed an audit of the information systems application used by the Division of Resolutions and Receiverships (DRR) to comply with the least cost provisions[1] of the FDIC Improvement Act of 1991 (FDICIA). This application includes the Least Cost Test; the optimization software package, *What's Best!;* and, the Insurance Determination Cost Calculation model. Collectively, these systems will be described as the Least Cost Test model (LCT model). The objectives of the audit were to determine whether the LCT model (1) operated as designed and (2) contained adequate controls to ensure complete and accurate results. Additional details on the audit scope and methodology are included in Appendix I.

BACKGROUND

DRR's mission is to plan for and resolve failing FDIC-insured institutions promptly, efficiently, and responsively in order to maintain public confidence in the national financial system. Within DRR, the Franchise and Asset Marketing Branch is responsible

[1] These provisions require the FDIC to resolve failing institutions in a manner that is the least costly to the deposit insurance funds of all possible resolution methods.

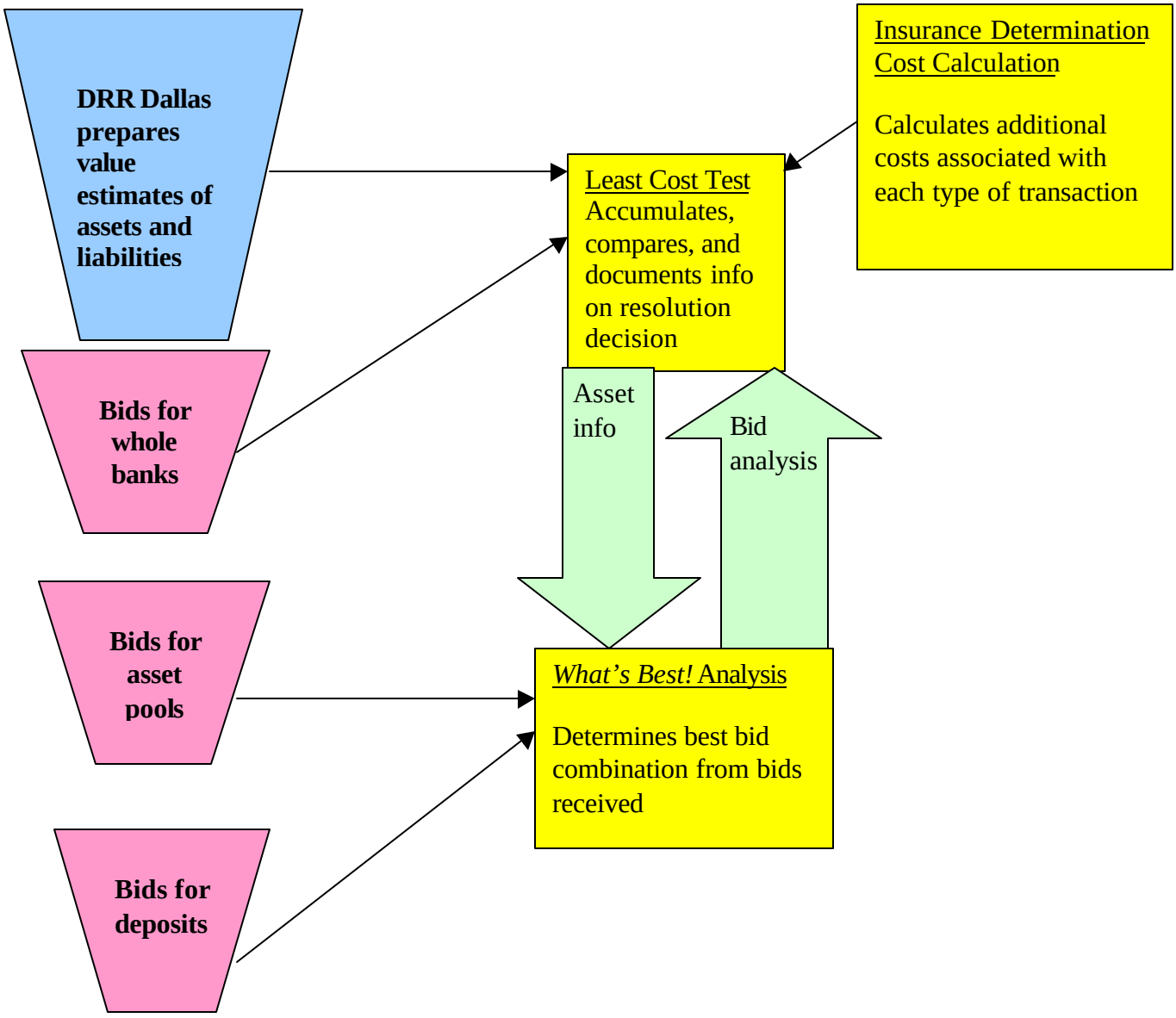
for resolving troubled financial institutions and selling assets at the least cost and highest recovery to the Corporation's insurance funds. The FDIC has various means to resolve a failing financial institution. Under FDICIA, the FDIC may exercise specified resolution authorities only where the chosen method is the least costly to the deposit insurance funds of all possible methods for meeting the Corporation's obligations. In addition, the FDIC has a strategic goal to ensure that institutions are resolved in the least costly manner in accordance with law. Therefore, the branch continues to develop, refine, and implement resolution policies, procedures, and strategies that minimize losses to the insurance funds.

In order to comply with the least cost provisions of FDICIA, DRR developed the LCT model, which tracks the FDIC's costs of liquidation and then compares these costs to other resolution options. Since 1991, the FDIC has been required to select the least costly resolution option and has refined its process over time. As currently structured, the LCT model contains three parts: the Least Cost Test, *What's Best!*, and the Insurance Determination Cost Calculation. The Least Cost Test is a series of Microsoft®[2] Excel-based spreadsheets that accumulates information on the failing institution and then compares the costs of various resolution options and documents the rationale for choosing one option as the least cost resolution.

[2] Microsoft is a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

The three parts of the model interface like this:

LEAST COST TEST MODEL



What's Best! is a commercial, off-the-shelf software program that evaluates multiple solutions and selects the optimal solution within the parameters established by the user. DRR began using the *What's Best!* optimization software in 1998 to evaluate the bids received for failing institutions. Previously, program staff manually reviewed and evaluated bids on failing institutions. Among the parameters established in *What's Best!* for evaluating the bids received for a failing institution are the prices established by DRR through the Asset Valuation Review (AVR). The AVR is prepared by the Franchise and Asset Marketing Branch of DRR in Dallas. The primary purpose of an AVR is to establish an estimate of the value of the institution's assets to the FDIC as receiver of the failing institution. The estimated value of a pool of loans offered for sale is used as the minimum price the FDIC is willing to accept from potential purchasers of failing institutions. *What's Best!*, as customized by DRR, selects from among the multiple bid combinations submitted for a failing institution's deposits and asset pools. Information on the winning bid combinations is transferred to the LCT model for comparison with the FDIC's cost of liquidating the institution. Information on a bid for a whole bank transaction is entered directly into the Least Cost Test.

The Insurance Determination Cost Calculation is a DRR-developed spreadsheet that estimates the additional costs of resolving the failing institution's liabilities in three basic resolution types. Such additional costs include travel costs for staff assigned to the closing, as well as overhead expenses associated with the resolution process. These costs are added to the FDIC's estimated loss under each resolution scenario for final selection of the least costly transaction. The Insurance Determination Cost Calculation was added to the LCT model in 1999.

The Least Cost Test templates, the *What's Best!* templates, and the Insurance Determination Cost Calculation template are all stored on DRR's shared drive for resolutions in a Least Cost Test template folder. At the beginning of the resolution process, copies of each template are made from this folder and then stored in a new folder specific to the failing institution on DRR's shared drive. When our audit fieldwork began, DRR had five Washington staff who entered information into the LCT model; however, reorganization during the audit doubled the size of the Washington staff who enter information into the LCT model.

Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources*, Appendix III[3], defines an application as the use of information resources (information and information technology) to satisfy a specific set of user requirements. It further defines adequate security as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or

[3] On October 22, 2001 the FDIC Legal Division issued an opinion that stated that OMB Circular A-130, Appendix III, partly applied to the FDIC. Among the parts of Appendix III that applied to FDIC was the requirement that FDIC implement and maintain a program to assure adequate security for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The FDIC Legal Division further opined that such programs are to be consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration, and the Office of Personnel Management.

modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

RESULTS OF AUDIT

The LCT model correctly determined the lowest cost resolution in both cases we reviewed. Therefore, we concluded the model is generally operating as intended. However, security controls for the LCT model needed improvement. Specifically, controls over access, software development, and changes were weak. For example:

- Access privileges were not always appropriately limited, including authority to modify the LCT model. Therefore, system changes could be executed without proper testing and approval.

- Software testing to demonstrate functionality was not documented. Therefore, the extent of testing and correction of test deficiencies was uncertain.

- Complete system software documentation has not been maintained. Therefore, software maintenance modification and recovery are impaired and may not be fully effective.

The FDIC has not designated the LCT model as a major application nor is it subject to the more rigorous security requirements associated with that designation despite the critical role it plays in the DRR resolution process. The model ensures that DRR complies with the statutory least cost provisions, processes highly sensitive information such as bids for the assets of failed institutions, and provides the basis for key FDIC decisions on resolving failed institutions. The Division of Information Resources Management (DIRM) has developed a new process for evaluating the sensitivity of FDIC systems that should be applied to the LCT model to determine if an upgrade in status is warranted.

LEAST COST TEST MODEL OPERATED AS DESIGNED

We judgmentally selected two resolution cases and reviewed the application of the LCT model in each case. We determined that in both cases the LCT model operated as designed. In each case, DRR selected the resolution option that was least costly to the insurance fund. In one case, only one bid was received, so the provisions of the *What's Best!* module did not apply. However, in the other case, the *What's Best!* module selected the best bid submitted. We noted discrepancies in both the Least Cost Test reports and the Insurance Determination Cost Calculation, but they did not affect the Least Cost Test decision.

Peoples National Bank of Commerce

The first resolution case we reviewed was Peoples National Bank of Commerce (Peoples), Miami, Florida, which was closed on September 10, 1999. The Franchise and Asset Marketing Branch generated balance sheet data for the AVR as of June 17, 1999. Information from the AVR was transferred correctly into the Least Cost Test. Because only one bid was received, there was no need to implement the *What's Best!* module of the LCT model. DRR just compared the bid to the cost of liquidation to determine which would be the least costly transaction. The OIG reviewed this comparison and determined that, by accepting the bid, DRR selected the least costly transaction.

Finally, the OIG reviewed the Insurance Determination Cost Calculation. DRR did not have any documented policies and procedures for the Insurance Determination Cost Calculation. We determined that outdated information on travel costs and benefits was used in the calculation. However, because the information was used consistently throughout the calculation, there was no effect on the results of the LCT model. Although current information would have decreased the estimated total loss to the FDIC, the single bid received was still less costly than the FDIC's cost of liquidation.

First Alliance Bank and Trust Company

The second resolution case we reviewed was First Alliance Bank and Trust Company (First Alliance), Manchester, New Hampshire, which was closed on February 2, 2001. The Franchise and Asset Marketing Branch generated balance sheet data for the AVR as of October 31, 2000. Information from the AVR was transferred correctly into the Least Cost Test. DRR received 21 bids from 5 different bidders for First Alliance. The OIG reviewed the *What's Best!* analysis and determined that DRR selected the least costly transaction. We noted user input errors and omissions in the LCT model documents, including the Insurance Determination Cost Calculation, but these did not affect the Least Cost Test decision process. DRR procedures required that the resolution case documents be reviewed by a Qualified Reviewer, a DRR employee designated to ensure that information is accurate and complete. Neither the preparer nor the Qualified Reviewer noted these errors during the resolution process.

In both the Peoples and First Alliance resolution cases, the errors noted on the LCT model documents did not invalidate the decision made by DRR as to which was the least costly resolution. However, these errors did point out the necessity to strengthen the review process. After we brought this weakness to the attention of branch management, they immediately developed a draft checklist to be used by the Qualified Reviewers to focus and document their reviews of the resolution cases. DRR also developed a user checklist as an added control to strengthen the review process and to assist the new members of the staff with completing the LCT model documents.

Recommendations

We recommend that the Assistant Director, Franchise and Asset Marketing, DRR:

(1) Formalize and implement the use of the Qualified Reviewer's checklist as planned and establish other controls to ensure that the documents generated by the LCT model to support the resolution decision are accurate and complete.
(2) Establish a process for periodically updating the underlying estimates in the Insurance Determination Cost Calculation to ensure decisions are based on the most current information available.

LCT MODEL CONTROLS NEED IMPROVEMENT

We reviewed both access controls and application software development and change controls[4] for the LCT model to determine whether adequate controls were in place. We determined that access to the model is not limited to those with a business need and that some personnel with access to the model had access beyond that needed to perform their jobs. Although their duties could be accomplished with read-only access to the LCT model, some DRR personnel had read, write, and change access to the LCT model. We noted several problems with the application software development and change controls. Specifically, DRR did not involve DIRM in the purchasing decision for *What's Best!* and, consequently, the software was not tested for compatibility with the FDIC's operating environment. There is also no record that the software was tested to ensure that it would operate effectively in complex resolution transactions. Additionally, there is little documentation of the development of the LCT model templates to use as a starting point when making future modifications. DRR also has not developed a system for requesting, making, testing, and approving changes to the LCT model templates. Finally, there is little security over the macros and formulas[5] included in the spreadsheets to prevent accidental or intentional changes. The users can change the macros and formulas included in the LCT model spreadsheets by directly overwriting the ones not protected. The system also allows users to make changes to the protected macros and formulas included in the LCT model spreadsheets by first removing the protection function and then editing those macros and formulas as desired. As a result, adequate security[6] is not necessarily achieved for the LCT model.

---

[4] Access controls limit or detect access to computer resources, thereby protecting these resources against unauthorized modification, loss, and disclosure. Application software development and change controls prevent unauthorized programs or unauthorized modifications to existing programs from being implemented.

[5] A macro is a set of commands and keystroke instructions combined by a user to perform a specific task. This differs from a formula, which performs a specific mathematical function.

[6] According to OMB Circular A-130, Appendix III, "adequate security means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls."

Access Controls

We obtained a list of employees with access to the LCT model. We reviewed their job responsibilities to determine whether access to the LCT model templates on DRR's shared drive was limited to appropriate personnel. Both the National Institute of Standards and Technology (NIST) standards and DIRM guidance recommended that access to systems be limited to those with a business need to protect the systems from unauthorized modification or misuse. The applicable sections of the NIST standards and DIRM guidance are included in Appendix II. Eighteen DRR employees have read, write, and change (RWX) access to the shared drive Least Cost Test template folder. Ten of these are DRR employees directly responsible for Least Cost Test activities, while the other eight are DRR employees who have access to the LCT model but no direct responsibility for Least Cost Test activities. In addition, a DRR contractor has access to the Least Cost Test template folder but not the entire shared drive. Our analysis of access to the LCT model templates is as follows:

- All eight users who are responsible for input into the LCT model have appropriate access.
- One of the four DRR managers with RWX access to the LCT model should have read-only access, commensurate with his responsibilities for analysis.
- Three Qualified Reviewers have RWX access to the LCT model templates. Only one of the Qualified Reviewers needs this level of access; the other two should have read-only access to the failing institution folder.
- Two support staff employees have RWX access to the LCT model, but their duties should require them to have read-only access to information specific to the failing institution and no access to the LCT model templates.
- The one field office employee who assists with modification to the Least Cost Test templates has an appropriate level of access on the shared drive.

We discussed our access concerns with the Assistant Director, Franchise and Asset Marketing, DRR and he agreed with our conclusions. Additionally, he has since taken action to limit the level of access as discussed above. DRR provided us with documentation from DIRM that access changes had been made.

Application Software Development and Change Controls

As noted previously, application software development and change controls prevent unauthorized programs or unauthorized modifications to existing programs from being implemented. These types of controls are normally included in a security plan. The LCT model is not a major application of the FDIC and is not required to have a security plan, although OMB Circular A-130, Appendix III, still requires the agency to ensure that security commensurate with risk is in place. During our review of documents and interviews with responsible program officials, we noted several types of problems in this area. They are as follows:

- When DRR purchased the *What's Best!* software in 1998, it did not involve DIRM in the process. Therefore, DIRM did not have the opportunity to test the software for

compatibility with the FDIC's operating environment. There was also no documentation that DRR had stress tested the program to determine if it would continue to operate effectively in complex resolution situations. Without knowledge of the purchase or access to the software, DIRM was unable to test the software's compatibility with the Corporation's operating environment until November 2000 and found compatibility problems that required DIRM to rescript the software. However, the rescripted program did not perform as DRR needed, which led to ongoing discussions between DIRM and DRR to resolve these rescripting problems. In the meantime, DRR decided to plan for an upgrade of its version of *What's Best!*, because the current version is not compatible with FDIC's planned upgrade of its computing operating environment. To complete the upgrade, DRR would purchase the upgraded version of *What's Best!* and develop new spreadsheets to use with the upgraded version. DRR has already purchased an upgraded copy of the *What's Best!* software and submitted it to DIRM for testing. This testing and implementation of the new version of *What's Best!* has to be completed before FDIC rolls out its upgrade of the computing operating environment, which is planned to be completed by the end of the first quarter of 2002.

- During the implementation of the original *What's Best!* software, Division of Research and Statistics (DRS) employees, with assistance from DRR program officials, developed spreadsheet templates used to document the *What's Best!* analysis. As part of the design process to facilitate a user-friendly system, DRS color-coded the cells to indicate into which cells bid information is entered, which cells are program-related, and which cells are used to evaluate data. The FDIC no longer employs the DRS employees responsible for designing the spreadsheet, and no one has documentation on how the spreadsheet was created in case modifications are needed during the upgrade of the *What's Best!* software.

- Neither DRR employees nor the DRR contractor primarily responsible for the Least Cost Test templates retains documentation of changes made to the Least Cost Test templates. There is no system for documenting the reason for the changes or the testing and approval of the changes. One DRR employee and the contractor know the password protecting the Least Cost Test template on DRR's shared drive, and the contractor changes the template at the direction of the DRR employee. Instructions are normally given by e-mail, but once the changes are made, neither the contractor nor the DRR employee retain any documentation about the changes made or the testing and approval of the changes.

- Using a copy of *What's Best!* provided to the OIG by DRR, we were able to edit the macros developed for transferring data between the Least Cost Test spreadsheets and the *What's Best!* spreadsheets even when the spreadsheets themselves were protected as part of the formatting. For example, we edited the macro transferring information about the asset pools offered for sale so that the wrong asset pool information was transferred to the *What's Best!* spreadsheets. Since *What's Best!* decides which is the best bid combination by comparing the bid price on a pool to the FDIC's AVR reserve price, transferring incorrect information on the asset pool would directly affect the *What's Best!* decision process. The macros tested within the LCT model appeared to be

operating as intended, although the controls over the macros could be strengthened. DRR management indicated that the contractor has already added password protection to the macros.

- When testing the Insurance Determination Cost Calculation, we discovered that some of the formulas within the template had been overwritten during a resolution in June 2000. These formulas automatically calculated staffing needs based on deposit base estimates developed during the Y2K process. Normally, users are directed to enter only institution identification and deposit account information; therefore, users in subsequent cases might not realize that the underlying formulas had been changed and would then be relying on results based on faulty assumptions. DRR promptly acted when the OIG brought this matter to its attention. The Insurance Determination Cost Calculation is being revised and will be added to the shared drive as a read-only file.

Recommendations

We recommend that the Assistant Director, Franchise and Asset Marketing, DRR:

(3) Periodically review access to the shared drive and the LCT model templates to ensure that employees have appropriate levels of access to the files.
(4) Develop and retain documentation to support the testing performed on the upgraded *What's Best!* software for compatibility with the FDIC's operating environment and performance in complex resolution solutions.
(5) Fully document the preparation of new spreadsheets or the modification of existing spreadsheets used in the operation of the upgraded *What's Best!* program.
(6) Establish procedures for requesting, making, tracking, testing, and approving changes to the LCT model.
(7) Ensure that the protection added to the LCT model macros is operating correctly.
(8) Incorporate steps in the resolution case review process to ensure that formulas are operating as intended and have not been overwritten.

DRR AND DIRM SHOULD REEVALUATE THE SENSITIVITY OF THE LCT MODEL

The LCT model was not designated as a major application within the FDIC and afforded the increased security that these systems receive. According to OMB Circular A-130, Appendix III, a major application is "an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." Appendix III of this report outlines the security requirements related to major applications. Although the LCT model was considered a mission critical system for Y2K, it was not designated a major application as part of the February 1999 Corporation Security Controls Program. The information analyzed and generated by the system provides the basis for the Corporation to meet its strategic goal to ensure that institutions are resolved in the least costly manner. Further, the Corporation is required by law to select the least costly resolution option, and the LCT

model has been established to provide a consistent methodology to support that requirement. Therefore, DRR and DIRM should reevaluate the LCT model for possible reclassification as a major application within the FDIC.

In February 1999, DIRM, using a Sensitivity Assessment Questionnaire (SAQ), evaluated the LCT model as part of the Corporate Security Controls Program. The SAQ was used in identifying major applications subject to enhanced security controls. At that time, based on information provided by DRR and the methodology used by DIRM to identify major applications, DIRM did not identify the LCT model as a major application of the FDIC. The rating scale used with the 1999 SAQ questionnaire evaluated the whole areas of system confidentiality, data integrity, and application availability. However, in June 2001, DIRM published a draft version of a revised SAQ that allowed the program users to evaluate the individual elements of each area. In addition, in response to OIG recommendations in another audit, the new SAQ provides more comprehensive information on how applications are classified under the guidelines and provides expanded criteria against which applications can be measured.

As noted previously, DRR is not currently required to have a security plan for the LCT model, because it is not designated as a major application. OMB Circular A-130, Appendix III, requires federal agencies to implement policies, standards, and procedures which are consistent with government-wide policies, standards, and procedures issued by OMB, the Department of Commerce, the General Services Administration, and the Office of Personnel Management. In 1996, NIST, part of the Department of Commerce, published a compilation of generally accepted principles and practices for securing information technology systems. This guidance recognized that planning at the system level would ensure appropriate and cost-effective security for each system. One area to be considered in the planning was a system-specific security plan. According to the NIST standards, the security plan should document the rules for development and operation of the system. According to NIST, a fully documented security plan addresses access controls and application software development and change controls to ensure that appropriate security controls are specified, designed into, tested, and accepted in the application.

Recommendations

We recommend that the Assistant Director, Franchise and Asset Marketing, DRR and the Assistant Director, Information Security Staff, DIRM:

(9) Apply DIRM's revised SAQ procedures to the LCT model and determine if a reclassification of the LCT model is warranted. The results should be forwarded immediately to the Office of Inspector General and the Office of Internal Control Management for follow-up.

(10) Develop a security plan for the LCT model as described in OMB Circular A-130, Appendix III and the guidance developed by NIST for generally accepted principles and practices for securing information technology systems.

CORPORATION COMMENTS AND OIG EVALUATION

On October 23, 2001, the Director of DRR and the Acting Director of DIRM provided a written response to the draft report. The response is presented in Appendix IV to this report.

The Corporation generally concurred with recommendations 1 through 8. These recommendations will remain undispositioned and open for reporting purposes. With respect to recommendations 9 and 10, which are also undispositioned and open, we have requested that the Corporation notify us of the results of its application of the revised Sensitivity Assessment Questionnaire and any subsequent changes to the security plan for the LCT model.

While the responses generally agreed with the OIG's recommendations, both DRR and DIRM noted that the LCT model is not currently a major application of the FDIC and therefore is not subject to the security plan provisions of OMB Circular A-130, Appendix III. The final report was modified to address their wording concerns with the draft report and to clarify the OIG's intent to recommend that security controls, commensurate with the risks associated with the LCT model, be implemented.

APPENDIX I

SCOPE AND METHODOLOGY

We selected two resolution cases for our review of the LCT model and the work performed by the DRR Washington staff. Each of the cases we reviewed represented the most current version of the LCT model at the time of the failure. We did not review the AVR process conducted by the DRR Dallas staff because a separate audit is in process.

We reviewed the resolution case files associated with the failures of Peoples National Bank of Commerce (Peoples), Miami, Florida, and First Alliance Bank and Trust Company (First Alliance), Manchester, New Hampshire. We judgmentally selected these institutions from the universe of 20 failures since 1997. As mentioned in the Background section of this report, DRR refined the resolution process over time by adding *What's Best!* and the Insurance Determination Cost Calculation and revising the spreadsheets included in the LCT model. We selected Peoples because this was the first resolution case that incorporated the Insurance Determination Cost Calculation component into the LCT model.

We selected First Alliance because it was the most recent resolution case completed during our review. By reviewing this most recent resolution case, we ensured that our review included DRR's most current LCT model and resolution process. Additionally, because DRR offered a variety of resolution options for First Alliance, the variety of bids received encompassed most types of resolutions available for offer by DRR.

In order to determine if the LCT model operated as designed, we

- obtained and reviewed DRR's draft Least Cost Test manual and draft Resolutions Policy manual as well as the Least Cost Test instruction sheets for established procedures and guidance,
- compared the information in the AVR report to the data manually entered into the balance sheet of the Least Cost Test and verified the accuracy of the data,
- compared the information from the original bid documents to the data manually entered into the *What's Best!* spreadsheets and verified the accuracy of the data,
- compared the information on the best bid combinations selected by the *What's Best!* analysis to the data electronically transferred to the Least Cost Test and verified the accuracy of the data,
- compared the information on the original bid to the data manually entered into the Least Cost Test and verified the accuracy of the data if no *What's Best!* bid analysis was performed during the resolution process,
- recalculated the Least Cost Test comparison sheets to verify the mathematical accuracy of the worksheets, and
- confirmed that the least costly resolution was selected by DRR.

In addition, to ensure that the *What's Best!* component operated as designed, we

- reviewed the sample case used by DRR in its training process,
- manually combined the bids received in the insured-only deposits case and the all-deposits case[7] and priced out each bid, and
- verified that *What's Best!* had selected the best bid combination for both the insured-only deposits case and the all-deposits case.

- For the Insurance Determination Cost Calculation, we
- determined whether the electronic transfer of information on staffing estimates was completed correctly,
- verified the average costs used in the calculation, and
- recalculated the cost of each type of insurance determination and verified the accuracy of the information used during the specific resolution process.

In order to evaluate the controls established by DRR for the LCT model, we

- reviewed the system application controls[8] associated with the LCT model;
- obtained and reviewed Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*;
- obtained and reviewed National Institute of Standards and Technology (NIST) Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*;
- obtained and reviewed Division of Information Resources Management (DIRM) directives, policies, and guidance regarding development, access, and security of FDIC systems for applicability to our audit;
- obtained, reviewed, and applied DIRM's draft guidance for SAQs to the LCT model to determine whether the LCT model could be designated a major application under the draft guidance;
- obtained a list of FDIC employees with access to the LCT model and reviewed it for appropriateness to job responsibilities; and
- tested the macros and formulas incorporated into the LCT model for security and edit controls.

Also, we interviewed personnel from DRR Dallas, DRR headquarters, DIRM, and DRS. We performed our work at the FDIC's offices in Washington, D.C. We conducted the audit from September 2000 through June 2001 in accordance with generally accepted government auditing standards.

---

[7] DRR may give potential bidders the option to acquire all deposit liabilities of a failing institution or just the insured deposit liabilities.

[8] Application controls are incorporated directly into individual applications and are intended to ensure completeness, accuracy, authorization, and validity of all transactions during application processing.

APPENDIX II

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) STANDARDS AND THE DIVISION OF INFORMATION RESOURCES MANAGEMENT (DIRM) GUIDANCE

Section 3.5.1 of Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* issued by NIST states:

> Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties.

DIRM guidance is contained in two FDIC Circulars, 1360.1 and 1360.15.
Section 6.c of FDIC Circular 1360.1 states:

> Access to sensitive information and information systems will be based on business needs.

Section 4.b of FDIC Circular 1360.15 states:

> Sensitive AISs [Automated Information Systems] and data shall be protected from unauthorized access, disclosure, and use. Access to sensitive systems shall be permitted only for business purposes, as approved by a supervisor and program manager, or their designee(s). Such access shall be terminated when it is no longer required or when access privileges have not been used for a predetermined period of time.

APPENDIX III

OMB CIRCULAR A-130, APPENDIX III, SECURITY REQUIREMENTS FOR A MAJOR SYSTEM APPLICATION

1) Assign Responsibility for Security

Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

2) Application Security Plan

Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic information resources management plan required by the Paperwork Reduction Act. Application security plans shall include:

a) Application Rules -- Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

b) Specialized Training -- Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules.

c) Personnel Security -- Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate.

d) Contingency Planning -- Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

e) Technical Controls -- Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST.

3) Review of Application Controls

Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A-123, *Management Accountability and Control* and the *Federal Managers' Financial*

Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

4) Authorize Processing

Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

FDIC

Federal Deposit Insurance Corporation
Division of Resolutions and Receiverships — Division of Information Resources Management

October 23, 2001

MEMORANDUM TO: Sharon M. Smith
Deputy Assistant Inspector General for Audits

FROM: Mitchell L. Glassman, Director [Electronically produced version; original signed by Mitchell L. Glassman]
Division of Resolutions and Receiverships

Carol M. Heindel, Acting Director [Electronically produced version; original signed by Wayne C. Gooding]
Division of Information Resources Management and
Acting Chief Information Officer

SUBJECT: Response to OIG Draft Report Entitled *Audit of the Least Cost Test Model* (Audit Number 00-724)

This memorandum will serve to respond to the issues and recommendations outlined in the draft OIG Audit Report, dated September 25, 2001.

General Comments:

On page 6, bullet three under **Results of Audit**, and on page 12, first paragraph under **Application Software Development and Change Controls**, the draft report incorrectly leads the reader to believe that an application security plan is required for the Least Cost Test Model (LCT). As the report correctly notes on pages 16 and 17, the LCT had been through the Sensitivity Assessment Questionnaire (SAQ) in 1999 and was determined not to be a major application. As such, there is no requirement for a security plan to be developed. The identified language on pages 6 and 12 should be revised to clearly indicate that this is not an issue of non-compliance by the FDIC and to be consistent with the language of pages 16 and 17.

The draft report indicates in the first full paragraph of page 17 that, "An appropriately developed security plan would require the Corporation to address our current control concerns." Based upon our review, the control issues identified by this report can be addressed in a timely, cost-effective manner by the actions specified in this management decision, without the need for development of a security plan.

(1) OIG Recommendation:
Formalize and implement the use of the Qualified Reviewer's checklist as planned and establish other controls to ensure that the documents generated by the

LCT model to support the resolution decision are accurate and complete.

DRR Response:
The Qualified Reviewer checklist has been formalized, implemented and used. It is a template located on our shared drive in the LCT folder and is password protected. It is also a part of our Least Cost Test Manual. The LCT checklist has been created for both the specialist who is completing the LCT and the qualified reviewer to aid them in correctly completing/reviewing all of the necessary documents. A memo to the Resolutions staff outlining the new procedures was sent on October 4, 2001.

(2) OIG Recommendation:
Establish a process for periodically updating the underlying estimates in the Insurance Determination Cost Calculation to ensure decisions are based on the most current information available.

DRR Response:
A process was established pursuant to the OIG recommendation. The Insurance Determination Cost Calculation Model and data will be reviewed during the first quarter of each year. New data will be gathered, and the programmer will update the defaults and other information in the model. Any changes will be reported to the Least Cost Test Policy Board. The LCT Manual was changed on October 16, 2001, to reflect the new procedures.

(3) OIG Recommendation:
Periodically review access to the shared drive and the LCT model templates to ensure that employees have appropriate levels of access to the files.

DRR Response:
A process was established on October 16, 2001, pursuant to the OIG recommendation. The Assistant Director, Franchise and Asset Marketing, DRR, will check with DRR Information Security in the first quarter of each year to confirm who has access to the LCT and determine if those people are the appropriate ones to have such access. Access can be altered, deleted or added at that time.

(4) OIG Recommendation:
Develop and retain documentation to support the testing performed on the upgraded "What's Best!" software for compatibility with the FDIC's operating environment and performance in complex resolution solutions.

DRR and DIRM Response:
One copy of "What's Best!" 5.0 (commercial version) was purchased and tested on June 26, 2001, by DIRM for compatibility with our operating system. DIRM rescripted the software to ensure compatibility, and the revised software was tested by DIRM and DRR. DIRM has retained the documentation of their testing

and rescripting. "What's Best!" 5.0 (commercial version) was "stress tested" by DRR to determine if the software would perform in a complex resolution scenario. "What's Best" passed the stress test, and DRR has retained documentation of the test. DIRM is now buying additional copies of the commercial version and upgrades of the professional version for DRR personnel who use the LCT model. Once the professional version is received, it will also be stress tested.

(5) OIG Recommendation:

Fully document the preparation of new spreadsheets or the modification of existing spreadsheets used in the operation of the upgraded "What's Best!" program.

DRR Response:

The spreadsheets that were created for "What's Best!" version 3.1 were used to stress test version 5.0. The software worked correctly with the original spreadsheets, and DRR has retained the corresponding documentation. (See response to # 4.) If, at some point, the spreadsheets need to be changed or new spreadsheets need to be created for use with "What's Best!" version 5.0, the preparation, modification and testing will be fully documented, and the documentation will be retained by DRR. These procedures are included in the LCT Manual.

(6) OIG Recommendation:

Establish procedures for requesting, making, tracking, testing, and approving changes to the LCT model.

DRR Response:

All changes are requested by e-mail from the LCT point of contact to the programmer and his supervisor. The programmer must obtain the password from the point of contact and then proceeds to make any changes. The point of contact tracks the change process and tests the changes for approval. After the changes are approved, the point of contact changes the password. The point of contact uses a spreadsheet to document the changes. These procedures are included in the LCT Manual.

(7) OIG Recommendation:

Ensure that the protection added to the LCT model macros is operating correctly.

DRR Response:

Password protection has been added to the LCT model macros. The LCT point of contact has the password and gives it to the programmer when a requested change to the model involves changing the macros. Once the change is complete, the password is changed by the LCT point of contact. The LCT point of contact periodically checks the password protection for the LCT macros. Documentation of the changes and testing will be maintained by the LCT point of contact.

(8) OIG Recommendation:
Incorporate steps in the resolution case review process to ensure that formulas are operating as intended and have not been overwritten.

DRR Response:
The Insurance Determination Model has been revised and is now a password-protected template. A step has been added to the Qualified Reviewer checklist to determine if the Insurance Determination Model has been correctly completed and to verify that the template has not been overwritten. These procedures are included in the LCT Manual.

(9) OIG Recommendation:
Apply DIRM's revised SAQ procedures to the LCT model and determine if a reclassification of the LCT model is warranted. The results should be forwarded immediately to the Office of Inspector General and the Office of Internal Control Management for follow-up.

DRR and DIRM Response:
Utilizing the Corporation's revised SAQ procedures, the LCT model will be evaluated by January 31, 2002. The results will be reviewed by the Least Cost Test Policy Board.

(10) OIG Recommendation:
Develop a security plan for the LCT model as described in OMB Circular A-130 and the guidance developed by NIST for generally accepted principles and practices for securing information technology systems.

DRR and DIRM Response:
The referenced OMB Circular A-130 requirement refers to a major system application. The LCT model was reviewed in 1999 and was determined not to be a major system application. If it is determined that the LCT model is a major system application, a security plan as described in Circular A-130 will be developed.

cc: Vijay Deshpande, Director, OICM
James Wigand, Deputy Director, DRR
Giovanni Recchia, Associate Director, DRR
Herbert Held, Assistant Director, DRR
Susan Whited, Assistant Director, DRR
Dean Eisenberg, Senior Internal Review Specialist, DRR
Wendy Hoskins, Resolutions and Receiverships Specialist, DRR
Janet Roberson, Deputy Director, DIRM
Wayne Gooding, Deputy Director, DIRM
Rack Campbell, Chief ITES Section, DIRM
James Lewis, Senior Computer Specialist, DIRM

Kenneth Jones, Section Chief, OICM
Penelope Moreland-Gunn, Manager Information Systems, DRR
Susan Seigman, Information Security Specialist, DRR