NATIONAL CREDIT UNION ADMINISTRATION

OFFICE OF INSPECTOR GENERAL

YEAR 2000
INTERNAL SYSTEMS REVIEW

OIG-993 MAY 19, 1999

Frank Thomas

FRANK THOMAS
INSPECTOR GENERAL

TABLE OF CONTENTS

Introduction

This is the second of the Office of Inspector General's (OIG) series of reports addressing the Year 2000 (Y2K) computer problem as it relates to the National Credit Union Administration (NCUA) and federally insured credit unions (FICUs). This report addresses the internal NCUA mission critical information systems. Because of the time critical nature of the Y2K problem, and in order to provide the NCUA Board with timely information, we are not making formal recommendations or asking for a written response. Rather, we are offering certain suggested actions as matters for consideration by the NCUA Board and agency management in this management report.

Other Y2K reviews in process include a review of FICUs progress in meeting the renovation phase milestone established by NCUA; and a review of credit union vendor status. Additional planned Y2K work includes a review of the progress of high risk credit unions.

Background

In November 1997, Chairman D'Amours provided testimony before the Senate Banking Committee's Subcommittee on Financial Services and Technology regarding agency progress in ensuring that the credit union industry and the NCUA are prepared to meet the Year 2000. This testimony indicated several years of effort by NCUA to modernize the agency internal information systems infrastructure.

NCUA's Y2K remediation plan included totally replacing the existing mainframe host, system software, database, and communications with new client/server architecture. This included replacing all the Agency's desktop workstations; refurbishing all the Agency examiners' laptop computers with more memory, larger hard drives, faster modems, and an entire new operating system and office automation suite; and rewriting every information system using the most current tools, techniques, and processes.

The December 1998 NCUA Congressional Update reported that "All of our internally developed systems are Y2K ready." There are seven internal mission critical systems. As of December 1998 NCUA stated that all seven systems were Y2K ready with none of the seven to be replaced, repaired (validated), or to be retired.

The OIG contracted with KPMG LLP (KPMG) in December 1998 to review the NCUA's seven mission critical internal information systems plus the Office of Corporate Credit Union's (OCCU) and PARS (payroll) systems. We added OCCU and PARS systems to the KPMG review because they appeared to be critical systems and had not been included with the seven identified mission critical systems. The seven NCUA mission critical systems are: SAP (accounting systems); AMAC (Asset Management and Assistance Center); ARIES (NCUA examination system); Call Reporting system (information from FICUs); OSCAR (primarily "back office" NCUA systems); Office Automation; and Telecommunications (now referred to as IT Infrastructure).

The Office of Management and Budget (OMB) has set the standards for Y2K project management and activities for the Federal Government. These standards include certifying that appropriate steps are taken on Y2K conversions, verifying the status of each sites' progress on Y2K via a quarterly report, and submitting a plan for accelerating progress on outstanding issues. KPMG's review was designed in part to compare NCUA's Y2K plan for Y2K project management and testing, at the time of their review, against the standards outlined above as well as those observed to be utilized at other clients.

Objectives

Our review objective was to provide the NCUA Board and management with an independent analysis of the Y2K testing compliance for each of the mission critical systems identified by NCUA and to provide recommendations for correction of noted deficiencies. All observations and items for management attention refer to the Y2K project status and activities as of the end of the fieldwork. The engagement was limited to interviewing appropriate Office of Technology and Information Services (OTIS) and other NCUA staff; reviewing information systems testing and compliance documentation; identifying any additional testing needed; and reviewing the Y2K project management.

Scope and Methodology

The review was initiated in December 1998 and fieldwork was completed in January 1999. The analysis included a review of the testing documentation for the following systems:

- SAP R/3
- AMAC
- ARIES
- Call Reporting system
- OSCAR
- Office Automation
- Telecommunications
- Office of Corporate Credit Unions (OCCU)
- PARS (payroll)

In order to accomplish the review objectives, KPMG performed the following tasks:

- Reviewed the testing methodology (where applicable) and compared it to industry practices and federal requirements;
- Reviewed the types of testing defined to achieve Y2K compliance and compared them to industry practices and federal requirements;
- Reviewed the actual test results and compared them to expected results to ensure that the testing accomplished stated objectives;
- Reviewed the actual test results and determined that all test cases were evaluated and that any discrepancies were noted, resolved and any necessary re-testing was performed; and
- Reviewed documentation maintained for testing performed and compared it to industry practices and federal requirements.

The contractor's final report is the basis for this OIG management letter report to the NCUA Board and management. KPMG's review of Y2K issues was not designed to, and does not provide any assurance as to whether Y2K issues which may exist will be identified; the adequacy of NCUA's Y2K remediation plans; or whether NCUA is or will be Y2K compliant.

OBSERVATIONS

NCUA has completed testing for each of its mission critical systems. The testing was performed in accordance with federal standards and industry practices. Testing documentation was found to be adequate to support the work performed. The review did not disclose any additional testing needed for the NCUA seven mission critical systems and two additional systems. NCUA is currently in the process of finalizing contingency plans to be implemented in the event of a disruption due to Y2K problems.

NCUA has taken precautions and actions to mitigate the risk of Y2K related failures on its internal mission critical systems. However, because of the unprecedented nature of the Year 2000 issue, its effects and successes of related remediation efforts will not be fully determinable until the year 2000 and thereafter.

Y2K project management oversight at NCUA includes both internal agency systems and individual credit union systems. The Director of the Y2K Project Office obtains information from the Office of Technology and Information Services (OTIS) regarding the status of agency systems. Also, the director obtains information from the Office of Examination and Insurance (E&I) regarding the status of credit union systems. Utilizing information from OTIS and E&I, the Y2K director provides periodic status reports to the NCUA Board and Congress regarding efforts and progress being made to ensure Year 2000 readiness at the agency and at credit unions. Because of the crucial nature of the project management function we decided to include a review of the adequacy of NCUA's oversight function. We have identified several observations for improving NCUA's Y2K project management.

Testing Performed in Accordance with Federal Standards and Industry Practices

NCUA began planning for Y2K compliance in 1995 and initiated its testing in December of 1997. At the completion of the fieldwork in January 1999, NCUA had completed testing for each of its mission critical systems. The fieldwork included the review of the test plan, test scripts, and test results for the seven mission critical systems, as well as two additional systems selected because of their critical nature. The NCUA testing methodology consisted of both date rollover and forced date changes. The testing was performed in accordance with federal standards and industry practices.

Test Documentation Adequate

The test documentation was found to be adequate to support the work performed. At the time of the review no additional testing was identified as being needed for NCUA's seven mission critical systems and two additional systems selected for review.

The following was noted with regard to NCUA's Y2K testing effort:

- The Federal Systems Integration and Management Center (FEDSIM) was engaged to evaluate SAP R/3 for year 2000 exposures and testing. FEDSIM was also responsible for developing documentation to support this effort;
- As suggested, NCUA utilized the format and substance of the FEDSIM documentation as a guide for the development of their final testing documentation; and
- All prior review comments related to OTIS test plans and compliance have been appropriately addressed (prior to this engagement KPMG had performed reviews at OTIS).

Y2K Project Management Oversight Could Be Improved

Project management oversight includes monitoring and reporting actions taken regarding internal agency systems and individual credit union systems. Overall Y2K project oversight is performed by the director of the Y2K Project Office. The director obtains information from OTIS and E&I and provides periodic status reports regarding internal agency systems and individual credit union systems to the NCUA Board and Congress.

The following observations present our views on how Y2K Project Management Oversight could be improved:

1. There is no formalized Y2K Project Plan (based on the General Accounting Office guide) that outlines the various components of the project and organizes and controls each project phase complete with milestone dates for completion of each phase. In addition, several testing/maintenance procedures were scheduled for the first and second quarter of 1999. We have no evidence that these procedures were included in the Y2K project test plan and that these plans were forwarded to the Project Office. These procedures include visiting all of the regional offices, submitting copies of the current Y2K database and soliciting feedback from those offices related to systems and applications not already included therein, testing those systems to ensure readiness and updating the database based on responses received.

2. There is no independent verification or validation of the accuracy and completeness of information reported to the Y2K Project Management Office. The Y2K project office function consists of only one individual. This individual is responsible for independent centralized management, control and oversight of the overall NCUA Y2K project and related reporting. Currently, the Project Office acts as a central repository for Y2K related information and documentation. Information is gathered at the office level and reported to the Y2K Project Office where it is compiled and forwarded to the NCUA Board and Congress. In its capacity as Y2K project manager for the field, E&I provides independent verification of data sent from the regions. OTIS provides information regarding internal NCUA systems to the Project Office for reporting to Congress.

Validation of the information presented in these reports independent of the program function (E&I and OTIS), is not performed. A lack of management and oversight processes and procedures could negatively affect project management activities and result in missed milestones and related system compliance failures.

3. While NCUA examiners have received formalized Y2K training, personnel with NCUA Y2K project oversight responsibilities have not received formal Y2K training to facilitate the effective performance of related responsibilities, specifically in the area of contingency planning. Most of the training obtained to date has been "on the job" and individual research and investigation. As a result, important aspects of the remediation effort may be overlooked and may hamper the Project Office's ability to effectively direct corrective actions. In addition, formal Y2K project management policies, guidelines and procedures have not been developed and implemented by the Project Office.

4. At the time of the fieldwork, we saw no evidence that a process for consistently identifying data exchanges had been developed and implemented. Each system programmer identified the data exchanges independently and without guidance from the project office. In addition, while we noted that there was an overall awareness of embedded systems, we saw no evidence that a separate plan for addressing embedded systems or an evaluation of the impact of failed embedded systems was prepared. The current systems inventory for NCUA did not include embedded systems and there was no estimate of the number of embedded systems available at the time of our review.

5. NCUA is currently in the process of finalizing contingency plans to be implemented in the event of disruption of operations due to Y2K problems. We would encourage NCUA to complete and test these contingency plans to reduce the potential impact of Y2K related failures.

MATTERS FOR CONSIDERATION

The OIG is suggesting the following actions as matters for consideration by the NCUA Board and agency management:

NCUA should continue efforts to finalize and implement its Y2K Contingency Plans.

- Management should consider documenting all phases of the Y2K contingency planning process, specifically identifying areas that have not been completed. The Plan should include a scenario- based approach designed to identify all potential failure sources, an action plan to address and correct identified failures, and a schedule for activation or testing of the Plan. These plans must include alternative methods for processing and contingency plan activation timeframes. Management should also define the level of testing to be performed to ensure that contingency plans are adequate and appropriate.

NCUA should implement steps to improve Y2K management and control within the Project Office function.

- Management should consider documenting all phases of the Y2K project, specifically identifying areas that have not been completed as outlined in the General Accounting Office guide. Further, a project plan should be developed for all projects related to Y2K to ensure that the Project Office is aware of the status of all projects.

- Management should consider evaluating the staffing of the Y2K Project Office to ensure that the Y2K project is properly managed, controlled and Y2K project status information is subject to continuous independent verification and validation. In this regard, management should consider the development and implementation of a process to perform an ongoing independent review and verification of the information submitted to the NCUA Board and Congress. This process will ensure that the information presented is accurate and consistent with the project plans for the affected areas. This verification should consider areas such as: consistency of metrics reported, level of effort expended to date, level of effort to complete tasks and resource allocation for the completion of defined tasks. Further, this reporting should be the responsibility of an area independent of the monitoring, managing and controlling effort.

- Management should consider providing formalized training to individuals with key Y2K responsibilities. The type of training sought should be directly related to the current status of the Y2K project. For example, contingency planning training would be applicable due to the fact that NCUA is in the process of finalizing those plans. In addition, the roles and responsibilities for the project office's managerial/oversight activities related to the Year 2000 project and activities should be formally defined and should include the update/modification of inventories on the Y2K database.

- Subsequent to the completion of the fieldwork, NCUA management indicated that inventories had been prepared of both data exchanges and embedded systems/chips. The Y2K Project Office should independently evaluate the accuracy and completeness of the inventories. Items should be listed by criticality, related testing (if needed) should be scheduled, and the inventories should be forwarded to the Project Office to be used in the Y2K project management effort.

NCUA should determine the appropriate level of additional testing that needs to be performed to ensure systems remain Year 2000 compliant if subsequent changes are made to the information system environment.

- Although NCUA has completed testing and implementation of all mission critical systems, it is important for NCUA to ensure that subsequent modifications and environmental changes do not nullify previous Year 2000 compliance.

- The risk associated with modifying a system after it is Year 2000 compliant, will vary depending on the timing and complexity of the changes. The more applications, programs, and interfaces affected by a specific change, the higher the risk to conversion and testing integrity.

- Business users and management both have critical roles for managing the risk of system changes after a system is considered Year 2000 compliant. They both need to evaluate the benefit of potential changes in the context of Year 2000 compliance, and balance the risk of making such changes.

- Once a system has been considered Year 2000 compliant, steps need to be taken to ensure Y2K integrity is maintained. Subsequent changes, including platform upgrades, software enhancements, or any system modification should be evaluated and approved with the understanding of the implications.