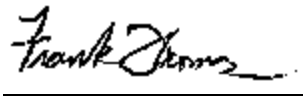
NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

Evaluation of Project Risks Associated with Upgrade to Comprehensive Human Resources Integrated System (CHRIS)

OIG-02-03 March 7, 2002



Frank Thomas
Inspector General

Released by:
William A. DeSarno
Deputy Inspector General

Auditor in Charge:
Tammy F. Rapp
Senior IT Auditor

Evaluation of Project Risks Associated with Upgrade to Comprehensive Human Resources Integrated System (CHRIS)

Table of Contents

EXECUTIVE SUMMARY

We performed a review of the National Credit Union Administration's (NCUA) planned upgrade to a new comprehensive human resources system. NCUA currently utilizes General Services Administration's (GSA) Personnel Information Resource System (PIRS). NCUA entered into an interagency agreement with GSA for the migration from PIRS to Comprehensive Human Resources Integrated System (CHRIS) currently scheduled to be implemented by the end of February 2002. Other than GSA, NCUA will be the first government agency to implement the customized version of CHRIS.

The purpose of our review was to determine whether NCUA has mitigated the project risks of a major HR system upgrade by performing appropriate analysis, planning, and monitoring. We contracted with Urbach Kahn & Werlin Advisors' Inc. to provide technical assistance. Our review was performed from October 31, 2001 through January 15, 2002.

The focus of this review was intended to provide reasonable assurance regarding the design and effectiveness of controls over systems and procedures. Our review identified several system migration weaknesses. These weaknesses could lead to overall increased project risk, NCUA needs/requirements not being met, the planned implementation timeframe not being met, increased security and system access risks, and expanding costs.

This report offers eight recommendations to help NCUA mitigate identified project risks.

- Ensure a structured process is in place for the development and acquisition of third party systems.
- Active OCIO involvement regarding the technical aspects of the evaluation process.
- Statements of Work should include specific description of deliverables, and provision for reasonable acceptance testing.
- Reevaluate the cost/benefits of CHRIS versus existing COTS packages now available.
- Implement a SDLC methodology that includes the role of key players who may be involved in the development and implementation processes.
- Define system security and access control requirements.
- Define user acceptance testing needs.
- Retain and review CHRIS system documentation.

These issues and the associated recommendations are discussed in detail in the attached report.

EVALUATION OF PROJECT RISKS ASSOCIATED WITH CHRIS

BACKGROUND

NCUA currently utilizes General Services Administration's (GSA) Personnel Information Resource System (PIRS), Payroll, Accounting, and Reporting System (PAR), Electronic Time and Attendance Management System (ETAMS) and limited functionality within the HR module of SAP. NCUA has entered an interagency agreement with GSA for the migration from PIRS to the Comprehensive Human Resources Integrated System (CHRIS) in early 2002.

Infrastructure: The modernized CHRIS/PAR software, and the platform upon which the software resides, will be owned and maintained by GSA. There is a single HR and payroll data center located in Beltsville, MD. CHRIS has been developed in partnership with current GSA clients and is designed to allow customization of the software to meet individual agency needs.

Hardware: Both the payroll and the HR application reside on IBM RS/6000 servers, located at the Lockheed Martin Data Center in Beltsville, MD.

Software: The CHRIS/PAR system was being developed and deployed as a client-server departmental system. However, the client conversion and implementation have been delayed until early 2002 in order to migrate to the web based version 11i of Oracle HR. The effect of which is to eliminate the client end of the product and implement a purely web-based application where the only requirements for NCUA use is a current internet browser, such as Microsoft's Internet Explorer or Netscape Navigator. The payroll system was designed and developed by GSA, using Oracle software. CHRIS is based on a moderately customized version of the Oracle Federal Human Resources software. Other COTS modules may be purchased to provide support for specific functions in the future.

Functionality: CHRIS will support all aspects of the personnel life cycle such as: recruiting, classification, staffing, compensation, benefits, training, EEO reporting, and personnel processing and management. The HR and payroll systems (CHRIS/PAR) will be fully integrated.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this review consisted of evaluating whether NCUA has mitigated the project risks of a major HR system upgrade by performing appropriate analysis, planning and monitoring.

In performing this review, the following areas were addressed:

- ✓ Review the current status of CHRIS implementation at NCUA
- ✓ Identify any federal and NCUA HR system requirements and whether those requirements are fulfilled by CHRIS
- ✓ Review the justification for the HR system conversion
- ✓ Identify the system life cycle costs, benefits anticipated, and risks
- ✓ Determine if agency identified all costs and tasks associated with the upgrade
- ✓ Determine contractual obligations with GSA for CHRIS
- ✓ Evaluate project team makeup
- ✓ Evaluate alternative options and decision process
- ✓ Identify any project milestones and plans for significant variances encountered
- ✓ Identify schedule and cost overruns and evaluate explanation of any overruns
- ✓ Review system test procedures performed and/or planned
- ✓ Review user training performed and/or planned
- ✓ Evaluate implementation and conversion plans
- ✓ Identify any security issues
- ✓ Review of system interfaces
- ✓ Evaluate the potential integration of CHRIS with SAP and other NCUA systems

We believe it is prudent to identify such risks for the record, under the premise that successful risk management ultimately depends on active, senior management commitment to:

a) the need to mitigate risks where possible, as early in the project's life cycle as possible; and
b) the need to accept and be accountable for clearly-defined risks that are not mitigated

SAP had been implemented as the back office application to process financials. In addition to the financial module, the OCIO produced the ability within SAP to create SF-50 and SF-52 forms as directed by the OHR. However, the use of these forms was never implemented within the NCUA OHR. In September 1997, the HR SAP implementation was put on hold due to an OHR focus shift to an Office of Personnel Management issue.

In May 1998, when the current Director of HR at NCUA was appointed, the need for a new personnel action processing system was revisited. The HR Director was not satisfied with the limited HR functions already implemented in SAP and requested an implementation that would institute all of the federal HR edits and checks, similar to those provided in the current system (PIRS). As of July 1, 1998 SAP had not made a decision regarding their commitment to federalized HR requirements within their commercial-off-the-shelf (COTS) package.

EVALUATION OF PROJECT RISKS ASSOCIATED WITH CHRIS

The OHR researched several options and chose the General Services Administration's (GSA) CHRIS system. CHRIS was selected because GSA would design CHRIS to interface with NCUA's current payroll system (PAR) thus eliminating the need to convert to a new payroll system. It is our understanding that conversion of the payroll system was a non-negotiable requirement of each of the other optional inter-agency vendors of Personnel Action Processing Systems. Since GSA was to design the system for it's own employees and would be the largest CHRIS client, NCUA believed GSA had a vested interest in delivering the system and, therefore, did not proceed with a formal requirements analysis.

The purpose of this memorandum is to present a statement of risks that we have identified during our review to date that, in our view, have not been mitigated by control techniques employed by the OHR team during their evaluation. We understand that our assessment may not address controls exercised informally, for example within the context of team meetings or discussions we did not attend. However, formal life-cycle controls are typically incorporated into key project management documents, and those we have had the opportunity to review do not appear to mitigate the accumulated risks we have enumerated below. Therefore, we must presume that these risks remain inherent in the project plan moving forward.

We conducted a review of NCUA's compliance with System's Development Lifecycle processes related to the CHRIS implementation. We do not provide assurance of the adequacy of the service provider's system. All work was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Our fieldwork was conducted at NCUA's Alexandria, Virginia Central Office from November 8, 2001 through December 14, 2001.

Planning Phase:

Our audit approach was designed to provide efficient, effective and timely procedures. The procedures performed during the planning phase were to ensure the audit work performed is sufficient to support our report. General procedures that we performed during the planning phase included:

- Obtained background information on the CHRIS implementation;
- Obtained an understanding of NCUA's SDLC methodology, control environment, as well as the controls inherent in CHRIS;
- Determined our general information needs; and
- Determined staffing needs and timing of fieldwork procedures.

The planning phase of the audit began with a detailed review of the service provider's contract with NCUA and other relevant available documents. During this initial review,

we documented our understanding of key contract provisions and determination of the effectiveness of the service provider's implementation of the contract.

Work program: The detailed work program documented our specific approach to the various review areas and included:

- The planned degree of reviewing of system development lifecycle;
- The planned extent of review procedures; and
- Other major planning decisions for areas which are of significance.

Determining specific review objectives and potential errors that could occur was the basis for the conduct of the audit. We planned our review procedures to achieve these objectives and to ensure we neither omitted any review procedures nor performed unnecessary ones. This work program became the basis for the design of our detailed review procedures. As procedures were performed and results obtained, the work program provided a framework for determining review judgments.

Service Provider Implementation: We performed interviews with critical OHR personnel to determine GSA's implementation of the CHRIS system. The procedures also included reviewing available documentation to determine:

- The availability of the CHRIS system developed to users of all required features and services;
- The availability of the system security policies and procedures developed by GSA; and
- The system lifecycle costs and benefits analysis.

Quality assurance: Establishing and maintaining effective security controls is an important responsibility of the management of the service provider. Effective quality controls are essential to achieving the proper conduct of the service provider under the NCUA contract with full accountability for its resources. Quality controls consist of those policies and procedures that GSA established to provide reasonable assurance that specific contract objectives are achieved.

We performed procedures to determine the availability of GSA's quality assurance program, including the system test plan and basic security policies to maintain quality assurance of the CHRIS system. The procedures we performed related to the quality assurance of GSA included interviewing critical NCUA OHR personnel and NCUA system security personnel to determine the availability of documented test plan and security policies.

FINDINGS AND RECOMMENDATIONS

We believe that NCUA would have benefited from a better-structured and better-controlled needs definition and product assessment process from the beginning. While we agree with OHR's assertion that conversion of the existing payroll system was unnecessary, we do not share the confidence of the OHR team that the selection process has led to a clearly superior decision and system for NCUA. In addition, we do not believe it is in NCUA's best interest to defer development and implementation of a security plan and risk assessment to the "post implementation" phase. Although NCUA can reasonably expect competent assistance from its service provider, we expect the costs of such reliance will continue to rise over time. Such costs could possibly rise to a point that narrows the cost|benefit gap between CHRIS and other comparable products regardless of payroll conversion requirements of the comparable systems. We anticipate that the implementation effort itself is likely to reveal where weaknesses in the acquisition model could have been more effectively addressed during the project's initial development. We have summarized the key risks as follows:

A. Management may be accepting an unreasonable level of overall project risk, due to the accumulation of potential weaknesses that have not been mitigated through strong project development controls;
B. NCUA user needs may not be specified in sufficient detail to ensure project success, due to over-reliance on GSA's ability to produce a system that will meet NCUA's requirements without a formal, independent needs analysis;
C. Lack of top-down management focus on enterprise architecture may increase project risk, perhaps due in part to insufficient OCIO and/or ITOC involvement, as well as resource constraints needed to focus on CHRIS initiatives;
D. Significant risk of project delivery due to repeated delays and variances in project milestones potentially leaving NCUA without the current Personnel Information Resource System (PIRs);
E. Significant security and access control risk due to lack of initial requirements analysis and documentation;
F. Significant risk of expanding costs, due to a possible 100 percent increase in processing fees by 2004.

EVALUATION OF PROJECT RISKS ASSOCIATED WITH CHRIS

This section summarizes the risks accumulated during the PIRS system replacement process.

1. A structured system development life cycle (SDLC) and acquisition process or policy should be developed and enforced.

Risk

In our view, there may be continuing residual risks to project success due to missing or deferred components of a well-structured SDLC-based system acquisition. The SDLC methodology should require that the solution's functional and operational requirements be specified. Regardless of whether a system is developed internally or obtained from a third party provider, a minimum level of controls are recommended to ensure that requirements are met, sufficient testing is performed, and appropriate security and controls are in place. In fact, NCUA recognized the importance of due diligence with third party providers and recommended in its Letter 01-CU-20 to All Federally Insured Credit Unions that credit unions perform a due diligence review when entering into agreements with third party service providers.

Recommendation 1

We recommended that NCUA ensure a structured process for the development and acquisition of third party systems. OHR did not, and was not required to, execute such a process. We further understand that a strict adherence to an SDLC methodology may not always be appropriate for all third-party SDLC projects. To allow for a more flexible SDLC approach, we recommend that the ITOC and OCIO agree and document the risk threshold limits that would require a strict adherence and approval of an SDLC project at NCUA. These risk threshold limits would define the amount of structure that is required for each SDLC project depending on the risk level per SDLC project (e.g., the greater the risk, the greater amount of SDLC structure that would be required by NCUA management). Approval of the risk threshold limits should be based on three primary factors: (1) the cost of the project, (2) the impact to on-going business operations and (3) systems security requirements.

Management Comments

Management officials did not believe the application of a SDLC in this specific procurement action was appropriate because NCUA did not develop a system. Regarding systems development, when OCIO converted the agency from a mainframe processing environment to a client/server architecture, it decided to look for an existing SDLC methodology to use in software development efforts. The agency decided for an

organization of NCUA's size, which does far more maintenance and incremental development, the best approach was to distill the key aspects of the Capability Maturity Model into the agency's local policies and procedures.

OIG Response

As previously stated in our report, we agree that a formal full Systems Development Lifecycle (SDLC) methodology may not be appropriate for every SDLC project. However, when committing to SDLC projects, NCUA management should quantify the risk to NCUA and assign an amount of SDLC structure that is required based on the level of risk. These risk threshold limits would define the amount of structure that is required for each SDLC project depending on the risk level per SDLC project (e.g., the greater the risk, the greater amount of SDLC structure that would be required by NCUA management). Approval of the risk threshold limits should be based on three primary factors: (1) the cost of the project, (2) the impact to on-going business operations and (3) systems security requirements.

We note that CHRIS was developed specifically for NCUA, which required modifications to the database tables and had data conversion needs. In addition, GSA is the first and only agency to implement CHRIS in the Federal government and NCUA would be first to implement the customized version of CHRIS. The due diligence that should have been performed is not unlike what NCUA requires from their member credit unions.

Furthermore, NCUA management should not wholly rely on the word of third-party vendors, whether these Federal agencies are small or large organizations within the Federal government. It is incumbent upon NCUA management to exercise their own due diligence in order to gain an appropriate level of assurance and minimize the overall risk to NCUA. To use an analogy, we all want the plane to land safely, but we also want to ensure that all reasonable safety precautions have been built into the process before takeoff. By taking the course of action of simply trusting GSA at their word, NCUA has taken on a much greater risk than necessary in order to implement CHRIS.

2. Active OCIO involvement is needed for SDLC projects.

Risk

We noted that OHR engaged various OCIO members in discussions regarding the SAP interface to CHRIS. However, technical and project risk may remain for NCUA due to OCIO's limited overall role in defining and managing CHRIS project initiatives.

Recommendation 2

OHR planners and personnel need to work closely with the ITOC and OCIO in order to retain guidance and analysis regarding the technical aspects of the evaluation process. In addition, OCIO personnel have the technical background to ensure adherence to NCUA IT security, access control and testing policies and procedures. We are not aware that the OCIO has been involved to this extent in the acquisition and testing of this mission critical system. In the future, OCIO should be actively involved and engaged at each phase of the SDLC process which includes: Concept, Requirements Definition, Detailed Design and Security Design, Development, Testing, Quality Assurance and Change Controls, and Implementation.

Management Comments

Management officials concurred with this recommendation.

OIG Response

OCIO was not actively engaged during the entire life of the CHRIS project. Although OHR retained an individual that previously worked for the OCIO, it is still important that OHR actively communicate the status of the project to OCIO on a regular basis. There are interdependencies within NCUA's systems architecture that could adversely affect systems operability or security without the active involvement of OCIO.

3. Formal Requirements Definition was not performed and detailed Statement of Work from GSA was Insufficient.

Risk

There may be continuing project technical and cost risk due to possible gaps in needed functionality that were either: (a) not disclosed, or (b) not completely worked through or reviewed at a detailed level. We believe that a risk to project success continues due to the failure of NCUA to establish a fully qualified universe of requirements and user needs. We are not aware that a unique NCUA needs definition was established as a basis for assessing whether NCUA requirements were met. Or, that such requirements are being used to determine whether GSA has delivered a core system that is, in fact, federally compliant with personnel action requirements. There also remains a risk that needs beyond the core personnel action requirements have not been defined or even recognized. The result of such a process is a system that may not meet the business needs, requirements and expectations of NCUA users. A Statement of Work should be detailed and include the specific description of deliverables, and provision for a

reasonable acceptance testing and may have mitigated these risks to NCUA's successful implementation of CHRIS.

NCUA relied on OPM's "The Guide to Processing Personnel Actions (Guide)" as the requirement's for the CHRIS project and has trusted in GSA to develop the system as needed. OPM's guide states in Chapter One, page 1-13,

"Follow carefully the instructions found in the chapter(s) appropriate for the action. The instructions cover only the Office of Personnel Management's requirements and may not include everything that your agency requires. Therefore, if your agency has its own processing instructions, you must follow them, as well. Because each personnel office may operate under different procedures, this Guide does not tell you who is responsible for each processing step."

We are concerned that this scenario has effectively been substituted for the level of structured needs definition that typically must be addressed specifically by candidate vendors, both to satisfy evaluation criteria and to be incorporated into contract language as leverage against future product acceptance. We do not believe that these goals were satisfied during the OHR's evaluation efforts although their approach likely did have the effect of "accelerating" the evaluation process.

There may be continuing project technical and cost risk due to possible gaps in needed functionality that were either:

a. not disclosed at all, or
b. were not fully worked through at a detailed level.

We noted in NCUA's Board Action Memorandum dated July 28, 1998 that there was a high-level summary of the *Federal Human Resources Information Systems Core Functional Requirements.* This document compares other Federal HR solutions with that of SAP. However, during our review OHR was unable to provide a documented account of NCUA's specific and unique systems requirements for CHRIS. This should have been provided to GSA during the Requirement Phase of the project. There remains a risk that NCUA's unique needs beyond the Core have not been defined or even recognized. The end result of such a process is a system that may not meet the user's business needs, user requirements and expectations.

In addition, we reviewed a document entitled Oracle Government *Human Resources Systems Requirements* dated February 28, 1997. This eight-page document outlines several business processes that GSA proposed to be delivered. However, during the course of our review, we noted that OHR had not received any documentation from GSA to ensure that these business process requirements were actually designed and

available to NCUA. OHR should have documentation supporting that these business processes requirements are actually functionally available from GSA prior to the implementation of CHRIS.

Recommendation 3

The Statement of Work should include the specific description of deliverables, and provision for reasonable acceptance testing.

Management Comments

Management officials do not concur. They believe the statement of work was adequate - CHRIS is a replacement HR system for PIRS, both of which were developed, implemented, and operated by GSA for federal clients.

OIG Response

We do agree that CHRIS may be functional for GSA and incorporate federal personnel processing requirements. However, NCUA management took GSA entirely on their word about the ability of CHRIS to perform as required by NCUA and did not request or receive any documented assurance from GSA that the final developed version of CHRIS was actually designed and functioning with all federal personnel processing requirements as well as NCUA's specific requirements. Therefore, NCUA management took on an ever increasing risk for NCUA by not performing an adequate level of due diligence in respect to SDLC processes.

4. Periodic reevaluation of the CHRIS business case is needed

Risk

CHRIS was originally scheduled to be operational for NCUA in 1997 with enhanced service offerings available to the Administration in early 1998. By July 28, 1998 when the BAM was presented to the NCUA board, the scheduled NCUA system conversion was already delayed to June of 1999. In July of 2000 the GAO issued its "Report to the Chairman, Committee on Government Reform, House of Representatives Information Technology Selected Agencies' Use of Commercial Off-the-Shelf Software for Human Resources Functions". In this report GAO stated that, according to GSA, the deployment delay was caused by: (1) a lack of maturity in the Oracle product relative to the HR needs of federal agencies, (2) a lack of skilled resources, and (3) GSA's decision to implement the system with internal staff. In October of 2000, GSA communicated to NCUA that a change in senior management (top CHRIS manager) took place. New management wanted to slow deployment and implementation in order

to determine how client implementation was to be conducted. Therefore, all client implementations, including NCUA's, were postponed into calendar year 2001. In December of 2000, GSA again communicated to NCUA that they had not yet received approval of the fiscal year 2001 budget for the CHRIS project. Thus GSA would be working with substantially less funding than anticipated which reduced the number of consultants working with GSA on the project. GSA again postponed implementation in this communication, but committed to bringing on external customers in Spring 2001. In May of 2001, GSA, again, discussed plans with NCUA to postpone implementation until the spring of 2002 in order to migrate to version 11i of the Oracle relational database management system. NCUA's go-live date is now scheduled for February 27, 2002.

We believe there remains a risk that the CHRIS system will not be fully implemented in the timeframe communicated by GSA, leaving NCUA at risk of not having a supported human resources information system. In addition, NCUA is uncertain of processing fees beyond the first two years, making it difficult to forecast future costs. According to OHR, the annual processing cost could rise from $60,000 to $120,000. It should also be noted that this cost estimate from GSA was verbal and there is no written agreement regarding future costs. Another point of consideration is that GSA may have only three clients utilizing the CHRIS system. Given this interagency client base, at some future date it may not be financially feasible for GSA to continue CHRIS service and support without considerable increase in annual fees of CHRIS users.

Recommendation 4

Though NCUA continually followed up with GSA regarding project delays, we could not verify that NCUA has reevaluated the business case regarding the GSA/CHRIS decision. NCUA should reevaluate the business case of implementing CHRIS on a periodic basis (e.g., annually) after implementation. This process will assist in identifying whether this system solution is still appropriate for the ongoing business strategy of NCUA. A systems business case review should focus on the detailed economics of the implementation and identify the estimated costs and benefits for NCUA over the life of the investment, as well as other business options that are available to NCUA. In addition, it may be beneficial for NCUA to determine if additional COTS packages are available that meet federal HR requirements and evaluate the benefits of implementing such a system considering both productivity gains and future cost savings.

Management Comments

Management officials concurred with this recommendation.

5. A structured SDLC project team should be implemented.

Risk

There may be additional risk to the overall success of the project due to a lack of a structured SDLC project team. For example, OHR has not interfaced with the CIO, NCUA's Security Officer, or GSA's Security Manager. Another concern brought to our attention is the lack of resource allocation in both the OHR and OCIO necessary to comply with sound best-practices SDLC procedures.

Recommendation 5

We recommend a SDLC methodology that includes the role of key players who may be involved in the development and implementation processes. Once senior management commits to the project, approval for the necessary resources is essential to ensure the involvement of key individuals or groups that adhere to a formal SDLC methodology. User management is responsible for systems requirements, acceptance testing and user training. The Project Manager ensures involvement from all affected departments, ensures the project adheres to standards set forth in the Statement of Work, while monitoring and controlling deliverables, costs and project timelines. The Security Officer provides guidance pertaining to suitable security processes that should be achieved and a Quality Assurance Manager confirms adherence to the requirements set forth in the formal requirements analysis and stipulated in the Statement of Work.

Management Comments

Management officials do not believe a strict SDLC model is appropriate for an organization of NCUA's size that does far more maintenance and incremental development. However, they do concur that active OCIO involvement is needed for systems development projects.

OIG Response

Regardless of how much structure is required for an SDLC project, it is essential that NCUA management ensure that basic internal control objectives are achieved in respect to project management. Some of these controls include and are not limited to; project management, systems security, and independent quality assurance management.

6. Detailed system security requirements and access control need to be defined.

Risk

GSA has not shared the security documentation pertaining to CHRIS with NCUA, however, GSA communicated that Oracle Business Groups will support the system security. When a NCUA user is assigned access to the system, the system security defines that individual works for NCUA, therefore he/she will only be able to see NCUA's data.
In order to maintain local control initially, the only persons with access to CHRIS will be the individuals at the Alexandria location who currently have access to PIRs. The Director of OHR will remain the only individual within NCUA with authority to approve personnel actions. Eventually NCUA plans to grant access to regional managers for generating requests for personnel actions and ad hoc reporting however the control details have not been thoroughly defined. GSA has not communicated to NCUA details pertaining to web based security however, NCUA believes in good faith that GSA will manage the security issues inherent in the web based version 11i of Oracle HR appropriately. We believe there is additional risk in NCUA's lack of understanding regarding the security features of the web-based application.

Recommendation 6

In addition to implementing technical and operational controls, testing needs to be planned and conducted to assure the security features effectively function by segregating users and protecting NCUA personnel action data.

Management Comments

Management officials concurred with this recommendation.

7. User acceptance testing needs to be defined.

Risk

As of our report date, NCUA has not received test plans from GSA however, NCUA has developed their own parallel testing plans. NCUA plans to manually check every account and test the most likely nature of action codes. Test parameters defined to the UKW SACteam include:

- Personnel transactions (A minimum of twenty records for each NOA will be tested) Specific NOAs and transactions to be tested included but are not limited to:

- Appointments
- Position builds and fast copies
- Reassignments
- Promotions
- Change to Lower Grade
- Details
- Pay (Agency unique)
- Separations
- Corrections
- Cancellations
- Awards
- Relocation Bonus

- Output Products
  - End of day processing (Validation reports, error reports etc.)
- Reports
  - EEO Extract
  - DESIREs
  - 113A & 113G
- Tables
  - Local table updates
  - Central table lookups and edits
- Interfaces
  - Payroll and Accounting Report (PAR) System
  - SAP
  - CPDF

Upon completion of the initial test cycle and certification of system specification by the OHR Automation Specialist, the OHR CHRIS Team will begin parallel operations for one-pay period. During parallel testing, sample personnel transactions will be processed and various output products will be reviewed for accuracy. Actions will be checked first to see if they meet the specifications requested and second to determine if the changes adversely impact other parts of the system. CHRIS results and reporting will be compared and reconciled to PIRS' corresponding data. Problems uncovered through testing will be documented and submitted to GSA CHRIS staff for resolution. Problems will be re-tested by NCUA OHR staff to complete the certification of CHRIS.

Although NCUA has scheduled parallel testing, there may be risk to the overall project success considering acceptance testing was not detailed in the Statement of Work and pass/fail criteria were not defined. NCUA assumes there will be signed user acceptance documents however this was not formally documented in the agreement with GSA. In addition, significant transactions not occurring during the pay period when parallel testing is performed may not be tested providing no assurance that these transactions will function properly for NCUA.

Recommendation 7

We recommend that NCUA detail user testing with GSA to include pass/fail criteria prior to beginning their own parallel test. NCUA should recognize that running a parallel test for one-pay period is an insufficient amount of testing because it may not represent significant transactions occurring in other pay periods. A minimum amount of due diligence would include reviewing GSA's test results. NCUA should review the following test results of the CHRIS system provided by GSA:

- Unit Testing
- System Testing
- Recovery Testing
- Security Testing
- Stress/Volume Testing
- Performance Testing
- Function/Validation Testing
- Regression Testing

Management Comments

Management does not concur. They believe that since CHRIS has been operational and in live production at GSA for over a year, the recommendation that NCUA request and review GSA's test plans, as detailed, is unnecessary.

OIG Response

We feel that it is necessary to re-state the need for NCUA management to conduct an adequate level of diligence in respect to overall systems testing. In addition, it is incumbent upon NCUA management to gain an appropriate level of assurance in order to minimize the business risk to NCUA. As a minimal requirement, NCUA management should have requested test results from GSA and not just relied on GSA's unverified assurances alone. Some of the requirements that should have been covered in a structured test plan include and are not limited to: Unit Testing, System Testing, Recovery Testing, Security Testing, Stress/Volume Testing, Performance Testing, Functional/Validation Testing, Regression Testing and User Acceptance Testing.

8. Data integrity controls need to be defined.

Risk

NCUA has been scrubbing current data and applying edits appropriate to CHRIS. During parallel testing, NCUA will manually check data to ensure accuracy of GSA's

initial data load and reconcile personnel action transactions. GSA has informally communicated to NCUA that Oracle Audit will be implemented to track system changes although NCUA has no verification of this or plans for testing the audit trails provided.

NCUA does not have assurance from GSA regarding control of transaction and transmittal logs or the identified audit trails. UKW Advisors, Inc. was not able to determine if these audit logs will be available for NCUA's review and/or testing. Such controls may be vital to ensuring the integrity and validity of NCUA personnel action data. Should system changes (either operating system, Oracle database or application program(s)) occur that affect NCUA personnel action data outside of normal user transactions, NCUA may not have sufficient audit trail to track and reconcile changes.

Recommendation 8

In order to determine the reliability of computer-processed data, the user should understand system controls which include both general and application controls. Documentation of a well-controlled system should be complete and current. We recommend that NCUA retain and review CHRIS system documentation. In addition, NCUA should request and review documentation from GSA pertaining to error correction procedures, transaction logs, transmittal logs, and audit trails as well as the accessibility of this information to NCUA personnel. OHR has indicated that they will have paper trails for a full reconstruction. However, the manual reconstruction of these documents is a voluminous task that will create labor inefficiencies and could result in human error. It is more efficient and practical for NCUA to pre-define automated controls and review the systems transaction logs.

Management Comments

Management does not concur. They believe the core Oracle HR product provides the appropriate audit trails and error correction procedures and logs necessary to provide the appropriate level of data integrity.

OIG Response

We understand that the core Oracle HR product provides audit trails and error correction procedures. However, NCUA management has not defined a process to review these logs to ensure that internal controls are built into the business process. Documentation of a well-controlled system should be complete and current. In addition, NCUA should request and review documentation from GSA pertaining to error correction procedures, transaction logs, transmittal logs, and audit trails. Furthermore, NCUA did not have assurances from GSA regarding control of transaction and transmittal logs or the identified audit trails. Each of these internal control areas should be included in the CHRIS project plan as normal due diligence.