OFFICE OF INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND
COMMUNITY SERVICE

OIG Letter Report Regarding Assessment of Project Risks Related to the Corporation for National and Community Service's Development of a Grants Management System

OIG Audit Report Number 02-22
February 4, 2002

Prepared by:

KPMG LLP
2001 M Street, N.W.
Washington, D.C. 20036

Under the Corporation for National and Community Service
Purchase Order # 200107180002
GS Contract # GS-23F-8127H
Task Order # 00-01

This report was issued to Corporation management on March 29, 2002. Under the laws and regulations governing audit follow up, the Corporation is to make final management decisions on the report's findings and recommendations no later than September 30, 2002, and complete its corrective actions by March 29, 2003. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

Letter Report Regarding Assessment of Project Risks Related to the Corporation for National and Community Service's Development of a Grants Management System

OIG engaged KPMG LLP to prepare a project risk management assessment of the Corporation's contractual initiative to develop an integrated grants management system (known as E-SPAN) capable of providing comprehensive financial information for all grants and cooperative agreements. This independent risk assessment of the project's management practices employed a five-part methodology that considered: (1) assessing the inherent risks; (2) understanding the controls in place; (3) assessing the effectiveness of the controls; (4) identifying control weaknesses; and (5) deducing and reporting residual risk. OIG has reviewed KPMG's assessment methodology, findings and recommendations and concurs with them.

The assessment concluded that the Corporation has adequately managed the E-SPAN project and found that the current level of residual risk is low except in a few medium risk areas. The analysis identified three areas that require additional management attention and makes the following recommendations:

(1) The Corporation should develop or adopt a specific quality assurance and testing methodology for the new E-SPAN system that is consistent with applicable standards and accepted best practices. It should also develop performance criteria and guidelines that specify how a third-party provider of quality assurance and testing services will be required to carry out its activities, document its observations, and communicate its recommendations.

(2) The Corporation should document criteria for testing specific application security and internal controls to be used for both initial and on-going quality assurance and validation testing of E-SPAN.

(3) The Corporation should develop a system life cycle management strategy and plan for operation and maintenance of the E-SPAN system throughout its expected operational lifespan while personnel with detailed knowledge of the system design are still available.

OIG understands that the Corporation plans to complete the development of E-SPAN and achieve initial operational capability of the system in April 2002. As required by the Conference Report on the Corporation's appropriations for Fiscal Year 2001 under the National Community Volunteer Act, OIG will participate in the certification of the new grants management system after E-SPAN's development and testing are completed.

Office of Inspector General
Corporation for National and Community Service

Assessment of Project Risks Related to the Corporation for National and Community Service's Development of a Grants Management System

Table of Contents

KPMG

2001 M Street, NW
Washington, DC 20036

Telephone 202 533 3000
Fax 202 533 8500

February 4, 2002

Inspector General
Corporation for National and Community Service
Washington, DC 20525

At your request, KPMG LLP (KPMG) performed an assessment of project management risks associated with the Corporation's initiative to develop a new grants management system, E-SPAN. This assessment is a precursor to the ultimate certification of the system that must be performed in accordance with the conference report on Public Law 106-377. (The conference report requires the Corporation to certify, with the Inspector General's concurrence, that an adequate cost accounting and grants management system has been acquired and implemented, and that it conforms to all federal requirements.) This project risk assessment focused on understanding risks that would interfere with the Corporation's ability to complete the acquisition and implementation of a new grants management system, and, consequently, the ability to certify a new system, as required by the Congress.

In July 2000 the Corporation engaged STR LLC, a professional services company, to assist the Corporation in designing a grants management system. In January 2001 the Corporation again contracted with STR to develop and implement the new grants management software. The Corporation's Chief Information Officer (CIO), in a memorandum dated February 2, 2001, requested input on the design of the grants management system from the Office of Inspector General (OIG). OIG subsequently engaged KPMG to conduct an independent assessment of the project's risks.

This assessment focused on understanding inherent project risks, the effectiveness of controls, and the existence of risks that had a significant effect on past performance and will influence successful development and implementation of the new system, E-SPAN.

Results in Brief

KPMG reviewed documentation provided by the Corporation and met with Corporation management and STR personnel. KPMG feels that overall the E-SPAN project is adequately managed, and residual risk is currently low, except in a few medium risk areas. The areas that need heightened attention are all related to future stages in system development and implementation. They are associated with software integration testing, quality assurance practices and life cycle planning for the E-SPAN system:

- The Corporation does not have a specific methodology nor documented performance criteria for quality assurance and validation testing. It is recommended that the Corporation develop or adopt a specific quality assurance and testing methodology for the new E-SPAN system that is consistent with applicable standards and accepted best practices. It is also recommended that performance criteria and guidelines be developed that specify how a third-party provider of quality assurance and testing services will be required to carry out its activities, document its observations and communicate its recommendations.
- The Corporation has not documented criteria for testing and re-testing specific data integrity controls and application security controls to be used during the phased implementation of the new E-SPAN system and also at later points in the system's life cycle. It is recommended that the Corporation document criteria for testing specific application security and internal controls to be used for both initial and on-going quality assurance and validation testing of E-SPAN.
- The Corporation has not documented a system life cycle maintenance and operation plan for E-SPAN beyond the initial three months of system operation. It is recommended that the Corporation develop a system life cycle management strategy and plan for operation and maintenance of the E-SPAN system throughout its expected operational lifespan while personnel with detailed knowledge of the system design are still available.

Project Scope, Objectives, and Methodology

Scope: KPMG assessed the project management processes and risks associated with the Corporation's initiative to develop and implement a new grants management system, E-SPAN. E-SPAN is being developed by a contractor, STR LLC, under the supervision of Corporation management, and with the involvement of Corporation personnel.

This assessment was a precursor to the ultimate certification of the system that must be performed in accordance with the conference report on Public Law 106-377. The conference report requires the Corporation to certify, with the Inspector General's concurrence, that an adequate cost accounting and grants management system has been acquired and implemented, and that it conforms to all federal requirements.

Objective: The objective of the assessment was to identify and assess project management risk in the following areas:

1. Project management control processes, techniques and methodologies;
2. The inherent risks that could adversely impact the successful completion of the new grants management system; and
3. The Corporation's actions to mitigate those risks.

Methodology: The assessment relied on KPMG's standard methodology for conducting project risk assessments. KPMG's methodology is based on and compatible with various widely accepted standards, such as *Control Objectives for Information and Related Technology* (COBIT), the Project Management Institute's *Project Management Body of Knowledge*, the Software Engineering Institute's capability maturity models, and appropriate National Institute of Standards and Technology (NIST) standards.

To conduct the assessment, KPMG gained an understanding of the current grants management environment and the E-SPAN project in the following areas: background information, project management, business processes, people and skills, and technology and data. Thirteen management control areas, sometimes referred to as project management domains, were reviewed. KPMG employed a five-part project risk assessment methodology. Its steps included: (1) assessing the inherent risk; (2) understanding the controls in place; (3) assessing the effectiveness of the controls; (4) identifying control weaknesses; and (5) deducing and reporting residual risk back to the Corporation. Details about each activity are presented below:

1. Assessing the inherent risk associated with the E-SPAN project entailed evaluating risks that existed prior to the implementation of controls. The assessment of inherent risk relied on the project kickoff meeting, initial discussions with Corporation management, preliminary reviews of documentation, and knowledge gained from previously delivering services to the Corporation.
2. Understanding controls in place entailed determining how the Corporation and STR, its contractor, control the direction and progress of the E-SPAN project. Understanding controls focused on domains that are commonly understood to be part of disciplined project management infrastructure and will have an impact on how well scope, time, requirements, configuration, and quality are controlled.
3. Assessing the effectiveness of controls included reviewing the extent to which project management activities succeed at delivering results to the satisfaction of Corporation management.
4. Identifying control weaknesses involved observing where project management practices showed a gap, and the gap could have significant potential for negatively impacting the success of the development and implementation of the new grants management system.
5. Deducing and reporting residual risk back to the Corporation involved consolidating the understanding of controls and control weaknesses into a set of overall observations and recommendations. A risk rating of high, medium, or low was assigned to each pair of observations and recommendations to indicate the level of residual risk. In this rating scheme, high-risk issues, of which there were none, require immediate action; medium-risk issues deserve heightened management

attention; and low-risk issues can be dealt with through standard operating procedures.

Summary of Findings and Recommendations

The assessment resulted in three medium risk findings that are discussed below. These findings are also included in Appendix C, a summary of all observations and recommendations.

- **Finding 1: Quality Assurance and Testing.** The Corporation has worked closely with its contractor, STR LLC, to perform ongoing testing of E-SPAN during the system's development. In addition, Corporation management has stated they plan to contract with a third party to perform independent testing and quality assurance for E-SPAN. The Corporation has prepared a request for quotation (RFQ) for these services that includes high-level requirements. But, the Corporation does not have a specific methodology nor documented performance criteria for quality assurance and validation testing.

  The SEI capability maturity model for software engineering and COBIT specifically address the value of having general and specific guidelines for quality assurance and testing. COBIT detailed control objective PO11.2, for example, states: Management should establish a standard approach regarding quality assurance that covers both general and specific quality assurance activities." Furthermore, detailed control objective PO11.18 indicates management "should define and use metrics to measure the results of activities, thus assessing whether quality goals have been achieved."

  KPMG did not observe the existence of consolidated documentation that meets these standards and believes that lack of a specific quality assurance and testing methodology could lead to a higher likelihood of testing not detecting all potential problems, and also, of not being efficiently repeatable in the future.

  It is recommended that the Corporation develop or adopt a specific quality assurance and testing methodology for the new E-SPAN system that is consistent with applicable standards and accepted best practices, such as those established by CMM and COBIT. It is also recommended that performance criteria and guidelines be developed that specify how a third-party provider of quality assurance and testing services will be required to carry out its activities, document its observations and communicate its recommendations.

- **Finding 2: Testing Plan for E-SPAN Application Security and Internal Controls.** The Corporation has addressed the security of E-SPAN in its system development process, but has not documented criteria for testing and re-testing specific data integrity controls and application security controls during the phased implementation of the new E-SPAN system and also at later points in the system's life cycle.

  Standards that espouse the value of well-planned and documented testing of application security and controls include NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* (NIST 800-27) and COBIT. NIST 800-27 (principle 13) calls for providing assurance that a system is, and continues to be, resilient in the face of expected threats. COBIT detailed control objective M2.2, which says: "Operational security and internal control assurance should be established and periodically repeated, with self-assessment of independent audit to examine whether or not the security and internal controls are operating according to the stated or implied security and internal control requirements." This is complemented by detailed control objective AI5.10 (part of the high-level objective, AI5, covering installation and accreditation of systems) states, "Management should define and implement procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the residual risk."

  Because the implementation of E-SPAN is expected to extend in stages over approximately a year and a half, the ability to repeat key quality assurance testing steps when new software modules are integrated with operational ones will be essential. Lack of a clear, documented plan and criteria for testing specific E-SPAN application security and internal controls could lead to failure to detect control weaknesses.

  It is recommended that the Corporation document criteria for testing specific application security and internal controls to be used for both initial and on-going quality assurance and validation testing of E-SPAN. The criteria should encompass security and internal controls for the new grants management application, and other interfacing applications, such as Momentum.

- **Finding 3: E-SPAN Lifecycle Management and Support Planning.** An option in the Corporation's contract with STR provides for three months of operational support for E-SPAN. The Corporation has not documented a system life cycle maintenance and operation plan for E-SPAN beyond that initial three months of system operation.

OMB Circular A-130, *Management of Federal Information Resources,* requires government agencies to have an information system life cycle plan. Also, COBIT detailed control objective DS13.1 states, "IT management should establish and document standard procedures for IT operations (including network operations). All IT solutions·and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence."

Not having a plan for maintaining the software, controlling modifications and providing a controlled operational environment for the application could have a negative effect on the efficient, effective management of E-SPAN.

It is recommended that the Corporation develop a system life cycle management strategy and plan for operation and maintenance of the E-SPAN system throughout its expected operational lifespan while personnel with detailed knowledge of the system design are still available. The Corporation should ensure the plan is consistent with applicable life cycle management guidance in OMB Circular A-130.

Appendix A discusses the current grants management processing environment. Appendix B provides an overview of the E-SPAN system development project. Appendix C presents the assessment observations and recommendations.

We conducted our audit in accordance auditing standards generally accepted in the United States of America and the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Distribution

We provided a draft of this report to the Corporation. The Corporation's response to our report is included as Appendix D.

As required by the Government Corporation Control Act, this report is intended solely for the information and use of the United States Congress, the President, the Director of the Office of Management and Budget, the Comptroller General of the United States, the Corporation for National and Community Service and its Inspector General, and is not intended to be and should not be used by anyone other than these specified parties.

Felipe Alonso
Partner, KPMG LLP

Appendix A

Our Understanding of Current Grants Management Processes

This appendix provides an illustrative, high-level view of the Corporation's processes for the review and approval of grant applications, and the systems that are currently used by the Corporation in the grants administration process.

AmeriCorps, Learn and Serve, and State and Local Commissions Grants

The processing of a grant application begins when a new application from a state/local office arrives at the Program and Planning Integration (PPI) Office. This office distributes the applications to the appropriate Program and Grants Offices. In the Grants office, personnel manually assign each grant application a 10-digit grant number, and enter the grant application information into the Grantsbase system. Grantsbase is a small system used in the grants review process to generate grant documents and modifications, and track financial reporting for authorized National and Community Service Act programs.

The application itself is put through the Grant Application Review Process (GARP). The Program and Grant offices develop a report and recommendation for the Board of Directors. One of the criteria for a recommendation of approval is that the grant be within previously established budget limitations. When approved by the Board of Directors, the grant application goes back to the Program and Grants offices for negotiation with the grantee. The Program office then creates a Certification for Funding that requires the signatures of the Program Officer and Director. When signed, the Certification is sent to the Grants office. After the signed Certification of Funding comes back from Accounting, the Certifying Officer requests that a grant account be created and an obligation established in Momentum. A grants specialist manually enters the obligation in Momentum. Momentum subsequently connects to the HHS Payment Management System (PMS) to establish a grant authorization. The Grantee is able to draw grant funds within the authorized limits directly from HHS.

The current grants management processes intersperse manual and automated processing. The approval and authorization process requires forms to be downloaded, signed, and forwarded to the respective offices. There is an electronic interface between Momentum and HHS-PMS, but there is no electronic interface between Grantsbase and Momentum. Information about the initial grant also flows from Grantsbase to both the Web-Based Reporting System (WBRS), and the System for Programs, Agreements and National Service Participants (SPAN). The Grantsbase information aids in setting up the initial grant information for progress reporting in WBRS and for related trust accounts in SPAN. But, updated information on subsequent modifications to the grant is entered manually into these systems, and does not flow from Grantsbase.

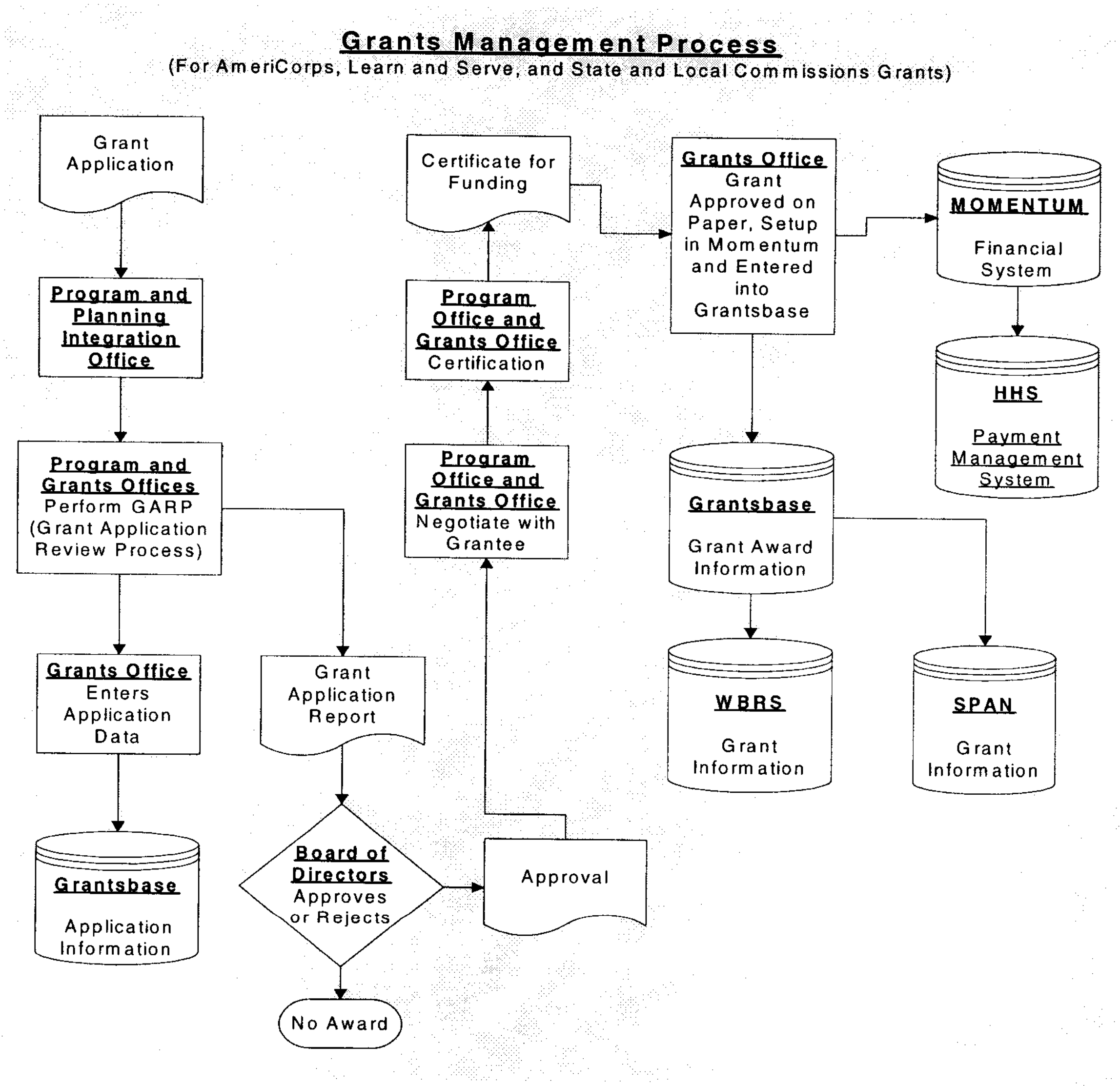
Grants Management Process
(For AmeriCorps, Learn and Serve, and State and Local Commissions Grants)
Grant Application
Program and Planning Integration Office
Program and Grants Offices Perform GARP (Grant Application Review Process)
Grants Office Enters Application Data
Grantsbase Application Information
Grant Application Report
Board of Directors Approves or Rejects
No Award
Approval
Program Office and Grants Office Negotiate with Grantee
Program Office and Grants Office Certification
Certificate for Funding
Grants Office Grant Approved on Paper, Setup in Momentum and Entered into Grantsbase
MOMENTUM Financial System
HHS Payment Management System
Grantsbase Grant Award Information
WBRS Grant Information
SPAN Grant Information

Figure A1: Current NCSA Grants Management Process Illustration

Senior Corps Program Grants

The processing of a grant application begins when a grantee submits a grant request to the CNS State Office. The grantee is often the State Commission which itself has multiple sub-grantees. The State Office Director, who has programmatic responsibility for the grant request, reviews the request, and signs giving his approval. It is then forwarded to the regional CNS Service Center.

The Service Center has financial management responsibility for the grant request. The Service Center has previously been given a budget for these types of grants by CNS headquarters. The Service Center Budget Officer verifies and signs off that funds are available. The Service Center Director then gives his approval by signing the request.

The request is then goes to one of several Service Center grants clerks, each of which works with multiple state offices. The actual document for the grant request is a Procurement Request form, because that is how the accounting system, Momentum, processes it. Coding information in certain fields differentiates a grant from Procurement Requests for supplies and services.

The grants clerk enters the grant request information to Momentum as a commitment. This signifies that that there has been "Grant Award Approval". The grants clerk then enters an obligation into Momentum. It creates a "Notice of Grant Award", and begins an automated process that transmits information to the HHS Payment Management System authorizing HHS to make payments to the grantee without further approvals by CNS. The Notice of Award document is printed by the system, and signed by the grants clerk.

The grants clerk next enters the grant request information into "Grants Module". Grants Module contains the standard Terms and Conditions that are used for all SCP grants. The Terms and Conditions are printed out to accompany the Notice of Grants Award.

The standard cover letter for the Notice of Grant Award is provided by headquarters as an MS Word document. It is printed out and placed together with the Notice of Award and the Terms and Conditions in a folder. Two copies of this set of documents are sent to the grantee. One set is sent to the State Office, and one set is retained in Service Center files.

Draw downs against the grant are monitored by using the Momentum Grant Status Report. The draw downs are considered to be an advance until the Grantee submits a Financial Status Report (FSR) explaining the actual use of the funds. Once an FSR or electronic equivalent are received, the funds previously advanced become an expenditure.

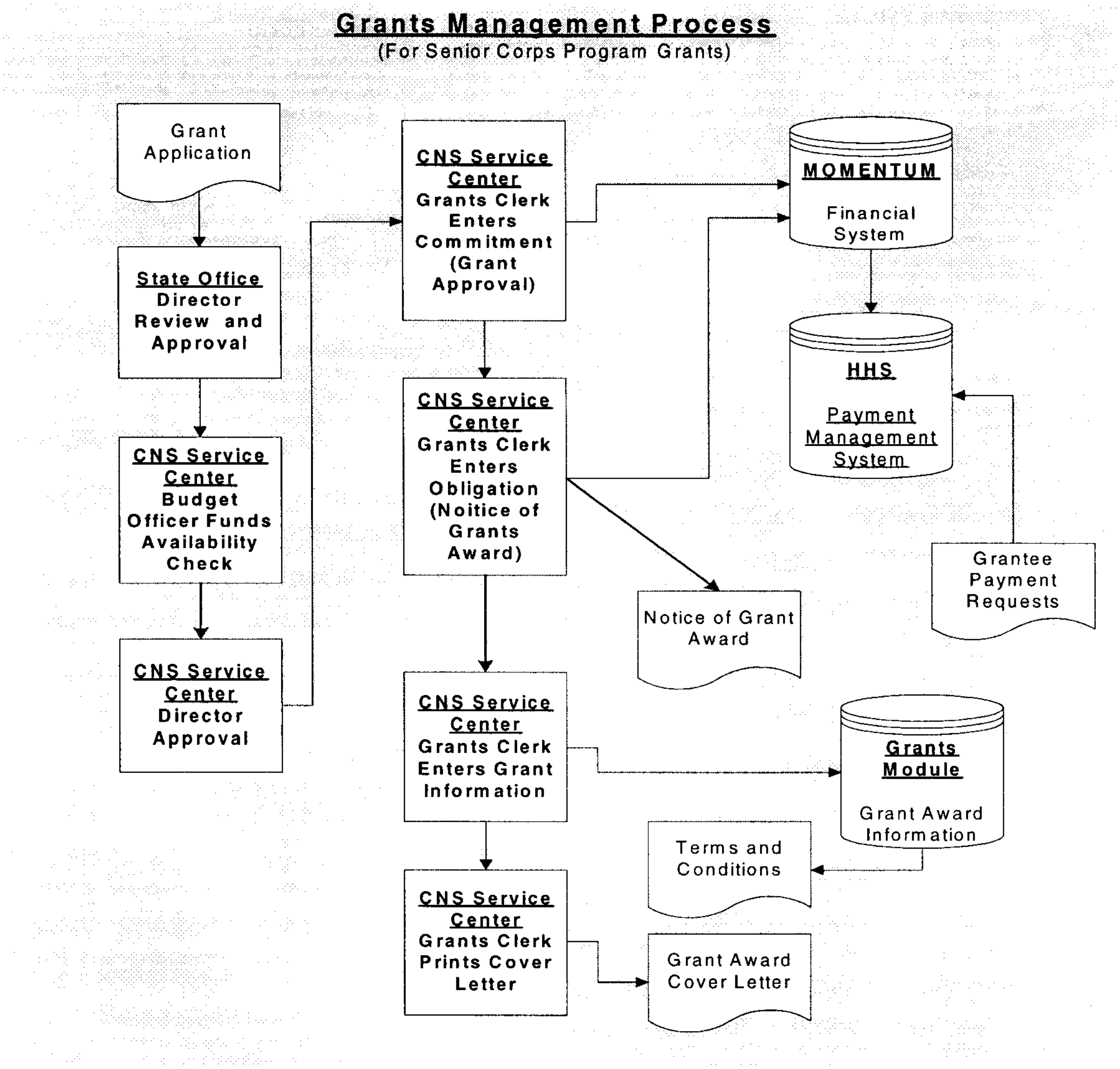
Grants Management Process
(For Senior Corps Program Grants)
Grant Application
State Office Director Review and Approval
CNS Service Center Budget Officer Funds Availability Check
CNS Service Center Director Approval
CNS Service Center Grants Clerk Enters Commitment (Grant Approval)
CNS Service Center Grants Clerk Enters Obligation (Noitice of Grants Award)
CNS Service Center Grants Clerk Enters Grant Information
CNS Service Center Grants Clerk Prints Cover Letter
MOMENTUM Financial System
HHS Payment Management System
Grantee Payment Requests
Notice of Grant Award
Grants Module Grant Award Information
Terms and Conditions
Grant Award Cover Letter

Figure A2: Current DVSA Grants Management Process Illustration

Appendix B

Our Understanding of the Grants Management System Development Project

Multiple pieces of legislation, enacted at different times, have established a variety of programs with different requirements, and different methods for administration. For this and other historical reasons, the Corporation has evolved a variety of processes and systems to manage its grants programs (i.e., AmeriCorps, VISTA, Learn ands Service America, and the National Senior Service Corps). The systems that have evolved to support the programs have different procedures and data file structures, and are not well documented. They require manual intervention, manual controls and rèdundant manual data entry. Inefficiencies and shortcomings, such as these, led the Corporation, with Congressional approval, to initiate the project to develop a new, integrated grants management system, E-SPAN.

E-SPAN will integrate the various formerly distinct systems and processes, and interface with Momentum. It will be a Web-based system developed using Oracle and Case tools that work with the Oracle8i software.

In July 2000, the Corporation selected STR to design E-SPAN. In January 2001, STR was also selected to develop and implement E-SPAN, with a "go live" date estimated to be approximately April 2002. A partial list of the tasks STR has performed or will perform for development and implementation of E-SPAN includes: conducting a detailed design review, developing forms and reports, mapping databases, conducting incremental testing, installing databases, conducting a complete system test with Corporation staff, developing training materials, training Corporation help desk and field staff, and developing a user's manual.

Although STR has the responsibility for system development and implementation, the Corporation plans to also contract with an independent third party for testing services. These services will provide the Corporation independent quality assurance and testing of E-SPAN.

Appendix C

Assessment Summary for the E-SPAN Project

The table below presents observations, recommendations, and a risk rating for each control area in the assessment.

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Project Sponsorship	As one of the largest software development undertakings in the Corporation's history, the E-SPAN project has sponsorship from senior management and congressional funding.	There are no recommendations for this control area.	Low	N/A
Steering Committee Leadership	Corporation senior management provides active oversight of the project, for example by participating in weekly status meetings. Through these meetings, as well as close involvement in the development effort, key managers stay abreast of new issues, outstanding issues, and project status.	There are no recommendations for this control area.	Low	N/A
Stakeholder Involvement	Program groups with a stake in the functionality that E-SPAN will deliver are represented in the design, development and implementation process. In addition, the Corporation has carried presentations about E-SPAN functionality to groups that will use the new system.	There are no recommendations for this control area.	Low	N/A

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Project Management Office	A project management office structure specific to E-SPAN is documented in the STR RFQ response. It includes procedures for having a project plan, staffing plan, budget, and project schedule. The Corporation and STR work closely together to carry out project management office duties, but a project management office similar to what might be part of a larger-scale application development and implementation effort has not been formally defined. STR uses various project management tools, including a finance and account system audited by DCAA. Introduction of an independent third-party test services provider into the E-SPAN project will introduce one challenge normally handled by a formal project management office, coordinating multiple vendors. Specifically, the Corporation has not documented a plan for coordinating collaboration between its stakeholders, STR, and a third party provider of quality assurance and testing services, in the context of identifying, documenting, and resolving any defects in the new grants management system that may be observed.	The Corporation should prepare guidelines for how the third party provider of quality assurance and testing services will document application development and implementation issues and will work with the Corporation and STR to resolve any observed defects in the new grants management system.	Low	N/A

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Project Team Composition and Skills	Corporation staff who are involved with the E-SPAN project appear to be senior professionals with an understanding of their functional areas. STR's personnel seem to possess sufficient technical qualifications, adequate experience, and a track record on complex projects. In discussions concerning the rationale for employing an independent third party to test E-SPAN, one reason offered concerned Corporation staff lacking the requisite complement of skill sets to carry out the effort as an internal project.	The Corporation should identify skill sets that will be required of both contractor personnel who will perform testing of E-SPAN and Corporation staff who will oversee this effort. The Corporation should ensure technical staff who will participate in testing possess adequate skills or receive training in key areas prior to the commencement of testing activities.	Low	N/A
Status Reporting	STR and the Corporation meet every week to discuss the status of the project. STR provides monthly status reports to the Corporation. A report identifies work planned for the next month and any problems, changes, risks, or requirements that may require the Corporation's attention. Documentation of status briefings and reports consistently track progress and the history of issues.	There are no recommendations for this control area.	Low	N/A

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Issues Management	Issues are logged, discussed, and resolved during the project and through weekly status meetings. Meeting summaries serve as a log of issues consideration and resolution.	There are no recommendations for this control area.	Low	N/A
Configuration Management	STR keeps code in an Oracle Designer Repository and takes steps to reuse code where possible. Adequate steps to maintain configuration information are being taken. The information tracked includes the purpose of the code, the location, the description and the author.	There are no recommendations for this control area.	Low	N/A

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Quality Assurance and Testing	The Corporation has worked closely with its contractor, STR LLC, to perform ongoing testing of E-SPAN during the system's development. Testing requirements are built into STR's responsibilities, and the stepwise development approach being taken for E-SPAN incorporates incremental testing and other testing efforts. In addition, Corporation management has stated they plan to contract with a third party to perform independent testing and quality assurance for E-SPAN. The Corporation has prepared a request for quotation (RFQ) for these services that contains high-level requirements. But, the Corporation does not have a specific methodology nor documented performance criteria for quality assurance and validation testing.	It is recommended that the Corporation develop or adopt a specific quality assurance and testing methodology for the new E-SPAN system that is consistent with applicable standards and accepted best practices, such as those established by CMM and COBIT. It is also recommended that performance criteria and guidelines be developed that specify how a third-party provider of quality assurance and testing services will be required to carry out its activities, document its observations and communicate its recommendations.	Medium	Finding 1

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Application Security and Internal Controls	Application security and internal controls have been considered during E-SPAN development and have been a topic of importance in the effort. STR has made concrete recommendations for strengthening access control, and Corporation managers describe application security and internal control as areas of continuing focus. However, the Corporation has not documented criteria for testing and re-testing specific data integrity controls and application security controls to be used during the phased implementation of the new E-SPAN system and also at later points in the system's life cycle.	Because the implementation of E-SPAN is expected to extend in stages over approximately a year and a half, the ability to repeat key quality assurance testing steps when new software modules are integrated with operational ones will be essential. It is recommended that the Corporation document criteria for testing specific application security and internal controls to be used for both initial and on-going quality assurance and validation testing of E-SPAN. The criteria should encompass security and internal controls for the new grants management application, and other interfacing applications, such as Momentum.	Medium	Finding 2

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Knowledge Transfer	STR will develop user manuals and other necessary documentation by the completion of the project.	The Corporation should work closely with STR, as manuals are developed, to determine that documentation will satisfy the needs of end users. To this end, business groups should provide input during the development of manuals. Along with other "as built" documentation, an "as built" design document should be prepared by the contractor before the system is accepted. The "as built" design document should clearly show all system controls that ensure the security, privacy, and integrity of the data in the system (accuracy, completeness, timeliness, etc.).	Low	N/A

Figure C1: Project Risk Assessment Summary

Project Control Area	Observations	Recommendations	Risk Rating	Finding
Lifecycle Maintenance	An option in the Corporation's contract with STR provides for three months of operational support for E-SPAN. The STR support will include training on an as-needed basis, technical fixes, database changes, and documentation updates. The Corporation has not documented a system life cycle maintenance and operation plan for E-SPAN beyond the initial three months of system operation.	It is recommended that the Corporation develop a system life cycle management strategy and plan for operation and maintenance of the E-SPAN system throughout its expected operational lifespan while personnel with detailed knowledge of the system design are still available. The Corporation should ensure the plan is consistent with applicable life cycle management guidance in OMB Circular A-130.	Medium	Finding 3
Training	STR will provide training to Corporation staff, and also work with key stakeholders in a "train the trainer" capacity at key points during the project.	The Corporation should leverage training and training materials provided by STR into knowledge capital that will serve future training needs of Corporation field personnel and help desk personnel.	Low	N/A

Appendix D

Memorandum

CORPORATION
FOR NATIONAL
AND
COMMUNITY
SERVICE

To: Terry E. Bathen
Deputy Inspector General for Audit and Policy

From: David N. Spevacek
Chief Information Officer

Date: March 18, 2002

Subject: Audit Report 02-22, Letter Report Regarding Assessment of Project Risks Related to the Corporation for National and Community Service's Development of a Grants Management System.

We are pleased that the KPMG assessment found that the Corporation is adequately managing the development of the eGrants system and that the risks inherent in this effort, therefore, are generally low. We do not disagree with the findings noted in the review and welcome the opportunity to outline the steps currently being taken to mitigate those risks.

The Corporation has engaged a company, not involved in the development of eGrants, to design a testing program, develop testing scripts that can be used now and in the future, and perform independent testing. This contract specifically addresses the first two of the three described risks:

> The Corporation should develop or adopt a specific quality assurance and testing methodology for the new E-SPAN system...
>
> The Corporation should document criteria for testing specific application security and internal controls to be used for both initial and on-going quality assurance validation testing of E-SPAN.

The Corporation's quality assurance and testing contractor is currently developing a project plan and beginning to develop test scripts. We are working closely with that contractor to make sure that the product of this effort addresses the risks identified by KPMG.

KPMG's third finding is as follows:

> The Corporation should develop a system life cycle management strategy and plan for operation and maintenance of the E-SPAN system throughout its expected operational lifespan while personnel with detailed knowledge of the system design are still available.

The eGrants system was developed within the context of the Corporation's existing Structured Systems Development Life Cycle Methodology (Policy #378). All major systems development is done using the full selection of ORACLE development tools. All system functionality will be available and understandable to any software developer, even someone completely unfamiliar with the system. The SPAN system has been operating under this life cycle strategy for several years. The Corporation is revising its on going ORACLE support contract to include the expected additional ORACLE expertise required by this new system. Throughout the development of the system, the Corporation and the system developer have maintained a list of items that were not in the initial design but that need to be considered in the next version of the software. That list is the start of an on going maintenance plan. For the last nine months, the Corporation has had internal conversations about staffing and related on going costs of the system. The very difficult administrative funding situation of the Corporation has meant firm decisions have not been possible.

KPMG is correct, the Corporation needs to take all of the above and put it into a single plan that will be available to anyone, including outside auditors. We plan to develop such a plan in later this calendar year.

We would like to thank the Office of the Inspector General and the staff of KPMG for their professional attention and their thoughtful insights into development project.