Audit of NARA's Internal Control Program

OIG Audit Report No. 13-01

December 10, 2012

Table of Contents

Executive Summary

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) performed an audit of NARA's Internal Control Program (ICP). The Federal Managers' Financial Integrity Act (FMFIA) as well as the Office of Management and Budget's (OMB) Circular A-123, *Management's Responsibility of Internal Control* (Circular A-123), provide guidance for implementation of an ICP. These materials require agency heads to conduct ongoing reviews of controls and to annually evaluate and report on the systems of internal accounting and administrative control. The purpose of this audit was to evaluate (1) NARA's compliance with guidance contained in FMFIA and Circular A-123, and the adequacy of the agency's assurance statement, (2) NARA's progress towards development of a formalized and comprehensive ICP, and (3) the status of open recommendations made in prior year reports.

Our initial assessment of the agency's FY 2011 assurance statement, as conveyed in our October 14, 2011 memorandum, was NARA's statement underreported material risk associated with Electronic Records Management. The agency has consistently underreported material risks over the past five years for programs including Preservation and Processing and has not accurately reflected the breadth of risks in NARA's Information Security Program. Without an effective ICP, the Archivist of the United States' (AOTUS) annual assurance statement to the President and the Congress may not clearly reflect NARA's current internal control environment, including risks.

Despite concurring with recommendations from prior reports issued by NARA's OIG and the Government Accountability Office (GAO) regarding an ICP[1], NARA has yet to fully establish the program. Management has not implemented an ICP because of the (1) complex nature of the program and lack of understanding of the benefits of the ICP, (2) lack of attention to the ICP, and (3) lack of resources provided for the successful implementation of the program. NARA has also not implemented five of the recommendations identified in prior OIG reports on the ICP.[2] By not implementing the program, NARA is vulnerable to a variety of risks that may not be foreseen or mitigated and is not able to self-identify and appropriately manage significant weaknesses such as those identified in prior and current audits performed by the OIG. Additionally, NARA is not able to take advantage of the benefits that come with establishment of a well defined and developed program such as (1) improved decision making, (2) risk identification, management, and mitigation (3) opportunities for process improvement, (4) effective use of budgeted resources, and (5) strategic planning.

We are making one recommendation which we believe, once implemented, will address weaknesses cited in this review.

---

[1] Identified as enterprisewide risk management in GAO's Report, *National Archives and Records Administration: Oversight and Management Improvements Initiated*, *but More Action Needed* (GAO-11-15).
[2] Recommendations from OIG 09-14 and OIG 10-19 have not been implemented by the agency.

Background

The Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255, requires each agency to establish controls that reasonably ensure: (1) obligations and costs comply with applicable law, (2) assets are safeguarded against waste, loss, unauthorized use or misappropriation, and (3) revenues and expenditures are properly recorded and accounted for. In addition, the agency head must annually evaluate and report on the systems of internal accounting and administrative control.

The Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control* (Circular A-123), defines management's responsibility for internal control in Federal agencies. It provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control. OMB revised Circular A-123 in response to the Sarbanes-Oxley Act, effective in fiscal year 2006. This revision strengthened the requirements for management's assessment of internal control over financial reporting. The new requirements apply only to the 24 Chief Financial Officer Act agencies, thus exempting NARA from reporting pursuant to Section 4 of the FMFIA. However, NARA is still required to report on internal controls pursuant to Section 2 of FMFIA.

NARA Directive 114, *Management Controls*, establishes policy for improving accountability and effectiveness of NARA programs and operations by establishing, assessing, correcting, and reporting on management controls. NARA 114 defines responsibilities; defines the types of reviews that could be considered internal control assessments; identifies documentation that must be maintained in support of an internal control evaluation, and addresses the development and maintenance of management control plans. Among the responsibilities defined by this guidance, Office Heads are required to identify and analyze risk, and the Performance and Accountability Office (CP) is required to provide oversight, guidance, and assistance to NARA offices concerning implementation of the NARA internal control program.

Interim Guidance NARA 160-1 describes FY 2012 requirements for reporting to the Archivist on internal controls. This reporting must include the status of control monitoring and testing activities, the status of recommendations resulting from audits, management reviews, and contractor assessments; and information pertaining to risks (such as current, or potential Material Weaknesses, Significant Deficiencies, or Control Deficiencies).

Assurance statements and information relating to FMFIA Section 2, Section 4 (from which NARA is exempt), and internal control over financial reporting should be provided in a single FMFIA report section of the annual Performance and Accountability Report (PAR) labeled "Management Assurances." The section should include the annual assurance statement, summary of material weaknesses and non-conformances, and

summary of corrective action plans. Furthermore, FMFIA requires the Archivist to annually submit to the President and Congress (1) a statement on whether there is reasonable assurance that the agency's controls are achieving their intended objectives, and (2) a report on material weaknesses in the agency's controls.

Objectives, Scope, Methodology

The objectives of the audit were to evaluate (1) NARA's compliance with guidance contained in FMFIA and Circular A-123, and the adequacy of the agency's assurance statement, (2) NARA's progress towards development of a formalized and comprehensive Internal Control Program (ICP), and (3) the status of open recommendations made in prior year reports. Specifically, we (1) conducted interviews with appropriate personnel associated with development of NARA's ICP and (2) reviewed the status of open recommendations made in prior year reports. Also, to facilitate the submission of NARA's annual assurance statement, we performed a preliminary review of the assurance statement in October 2011.

This audit was conducted in accordance with generally accepted government auditing standards between October 2011 and September 2012.[3] These standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

[3] The audit was delayed due to OIG staffing shortages. The auditor originally assigned this audit left the agency and the audit was on hold until it was reassigned.

Audit Results

1. NARA has yet to establish an Internal Control Program.

Although Senior Management agreed to formalize NARA's ICP in 2010, the program has yet to be developed and fully implemented. This condition exists because management has not made the program a priority, nor provided adequate resources to establish the program. As a result, the lack of an ICP (1) leaves the agency vulnerable to a variety of risks that may not be foreseen or mitigated and (2) does not allow the agency to self-identify and appropriately manage or mitigate significant weaknesses such as those identified in the *Audit of the Management of Records at the Washington National Records Center* (WNRC) (OIG 12-02 and 12-05) and *NARA's Network Discovery and Assessment Audit* (OIG 12-11). [4] Also, without the program, the Archivist of the United States' (AOTUS) annual assurance statement to the President and the Congress may not clearly reflect NARA's current internal control environment. An ICP (1) will provide more effective leadership, strategic direction, and accountability in fulfilling NARA's mission, meeting objectives, and establishing clear lines of responsibility for results, (2) ensures adequate controls are in place to provide reasonable assurance that program activities are operating efficiently and effectively; reliable and timely information is obtained, maintained, recorded, reported, and used for decision-making; assets are safeguarded, and that programs are managed with integrity and in compliance with applicable laws and regulations, and (3) enables NARA to better prevent, detect, and mitigate instances of waste, fraud, abuse, and mismanagement.

According to Circular A-123, management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Additionally, the Government Accountability Office (GAO) *"Standards for Internal Control in the Federal Government"* provides the underlying rationale for an ICP. The Standards state, "A key factor in helping achieve better ways to achieve agencies' missions and program results is to implement appropriate internal controls. Effective internal controls also help in managing change to cope with shifting environments and evolving demands and priorities."

---

[4] Audit Reports OIG 12-02 and 12-05 disclosed management controls were either missing, ineffective or inadequate to appropriately safeguard, secure, manage and handle records at WNRC. OIG 12-11 identified a lack of strategic planning with regard to the redundancy and resiliency and overall design of NARA's network. Internal control reviews, including risk assessments, prior to these audits could have identified some of the significant deficiencies identified in the OIG reports.

Prior Reports on NARA's lack of an Internal Control Program

In 2008, the OIG conducted an *Evaluation of NARA's Management Control Program* (OIG 08-06). We identified weaknesses which were the result of the lack of familiarity with NARA 114, *Management Controls*, an incomplete understanding of internal controls, and management control plans which were improperly or too narrowly scoped. The 2009 report, *Evaluation of NARA's FY2008 Management Control Program* (OIG 09-14), revealed at the end of the FMFIA reporting period, September 30, 2009, (1) management had not yet completed action to close recommendations contained in the prior year's audit report; and (2) two program offices did not adequately monitor internal controls. Our last audit in 2010, *Audit of NARA's Internal Control Program* (OIG 10-19), found NARA (1) had not implemented any of the prior year recommendations, (2) had not fully complied with the requirements of Circular A-123 as there was no formalized ICP, and (3) would not be in full compliance with Circular A-123 until it identified critical functions, control and monitoring activities, and developed a formal risk management process.

After issuance of the OIG's report in 2010, GAO reported similar concerns regarding an ICP. GAO's report, *National Archives and Records Administration: Oversight and Management Improvements Initiated*, *but More Action Needed* (GAO-11-15), identified NARA had not established an enterprise risk management (ERM) capability, reducing its ability to anticipate future challenges and avoid potential crises. GAO recommended the AOTUS develop and assign responsibility and resources for an enterprisewide risk management capability that allows it to monitor its internal and external environments continuously and systematically to ensure NARA's senior staff and decision makers can appropriately and quickly assess threats and vulnerabilities stemming from enterprise risks. As stated in the GAO report, without an effective program of risk assessment and internal control, management may have less assurance that it is using organizational resources effectively and efficiently, or that agency assets and operations are protected. The report further noted as called for by the *Standards for Internal Control in the Federal Government*, agencies should continuously and systematically monitor their internal and external environments to anticipate future challenges and avoid potential crises.

NARA's management concurred with all of the recommendations in the prior OIG reports on Internal Control. Specifically, for the 2010 report, they agreed to formalize the ICP to include the five standards for internal control: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. The Action Plan for the report indicated a completion date of May 2011 for the ICP. In response to the report from GAO, NARA committed to roll out an enterprise-wide internal controls program that uses risk assessment as an integral part of managing and monitoring internal controls, (2) embed an awareness of risk factors throughout the organization as part of an ongoing, repetitive process, and (3) assign a NARA Risk Officer to manage the process, who will raise risks identified to the Leadership Guidance Team (LGT) or similar executive leadership group.

Performance and Accountability Office and the Internal Control Program Project Plan

Since issuance of the last OIG and GAO reports, NARA has made minimal progress towards establishing an ICP. NARA's internal control practices have fallen behind as they have not kept pace with government issued directives and other federal agencies. Specifically, while CP has taken actions to improve NARA's ICP, actions to fully implement recommendations from the prior OIG and GAO reports are needed (see Appendix A – Status of Prior Recommendations), including development and full implementation of the ICP. CP's Management Control Liaison stated the other remaining open recommendations will be resolved upon the revision of NARA 114, *Management Controls*, which cannot be completely revised until NARA's formal ICP is fully developed.

In 2010, CP developed a project plan to address the areas in which NARA was not compliant with Circular A-123. Although the plan was revised in 2012 (See Table 1 – Status of ICP Project Plan), it does not clearly outline all of the key activities required for the ICP to be compliant with Circular A-123 and fully operational.

The current approach for implementing the ICP is to roll out the program at one time for all programs and functions within the agency, which could be a potential problem. According to McKinsey & Company's report, *Strengthening Risk Management in the US Public Sector*, government agencies should roll out new risk-management approaches one process or area at a time. There are several advantages to this approach including, (1) convincing the broader enterprise that risk management need not be a bottleneck and can be a source for positive improvement and (2) early efforts to improve risk management will lead to lessons that can be applied in subsequent efforts.

In August 2012 our review of the project plan indicated many of the activities have not been completed or started. Some are scheduled for completion by the end of FY 2012, including identifying existing programs and functions; and developing criteria to determine criticality and risk of functions. The Director of CP indicated the remaining activities will be completed over a three year span with the ICP fully implemented by the end of FY 2015[5], but agency officials have not been involved in the process to formally acknowledge this plan.

---

[5] Based on review the ICP will only be fully implemented by the end of FY 2015 if departmental and additional CP resources are available.

Table 1: Status of Internal Control Program Project Plan (provided by CP)

Task	Expected Date of Completion	Status as of September 2012
Populate ICP database with Program, Program Owner, Function, Function Owner, Open Recommendations and Performance Measures for each office	Complete by July 31, 2012	Complete
Develop criteria/questions for determining criticality (high or low) and risk (high/med/low) for each function	Complete by July 31, 2012	Complete[6]
Vet populated database with offices – ask for program and function owner names where missing, ask for offices to review program and function alignment one last time	September 2012	Complete[5]
Offices use criteria/questions to rank the criticality and risk of each function	September 2012	In Progress
Processes, SOPs/IOPs, and Key Performance Indicators (KPI) internal to each office are added to the ICP database (making it more comprehensive and robust) on the basis of function criticality and risk	Starts October 1, 2012 (ongoing throughout FY 2013)	In Progress - Ongoing
Assurance Statement/Internal Control Reporting to be based on and reflective of each offices Program and Function hierarchy. Consistently structured reporting from quarter to quarter and year to year	Starts October 1, 2012 (ongoing throughout FY 2013)	Ongoing
FY13 Internal Control Test Plan developed around high criticality, high risk functions	Tests plans for FY 2013 developed by October 31, 2012	Test to be developed based on results of risk questionnaires

The approach outlined by CP for implementing the ICP will result in a sufficient program; however it cannot be brought to fruition unless there is more management involvement and additional resources provided. Many of the tasks included in the project plan have not been completed because of the (1) complex nature of the program and management's lack of understanding of the importance of an ICP, (2) lack of attention and commitment by Senior Management, and (3) lack of resources provided for the successful implementation of the program.

Complex nature of the program and lack of understanding
Implementing an ICP is a difficult challenge because most NARA stakeholders (i.e. Senior Management, Program Owners, and Function Owners) do not have a basic understanding of (1) risk management principles, (2) the purpose of the ICP, and (3) the benefits to the agency of a risk management approach. As a result, managers do not adequately or consistently monitor controls associated with their programs or understand the risks to their programs and how to mitigate those risks. It will remain a challenge unless management communicates its commitment to the program and provides training to all stakeholders involved in the process. Currently, there is a lack of communication (e.g. Risk Management Policy) (1) of NARA's commitment to risk management and (2) to define key principles, roles, responsibilities processes, and common terminology.

---

[6] The tasks for Information Services need to be redone due to the recent organizational restructure and rewrite of NARA 101. Additionally, the Office of Innovation needs to be completed because it was only recently established and functional statements have not been finalized.

According to a report by the IBM Center for The Business of Government, *Managing Risk in Government: An Introduction to Enterprise Risk Management*, "educating a workforce unfamiliar with enterprise risk management terminology and concepts is a key issue for leading enterprise risk management activities." While CP recognizes the need, a training plan has not been developed or fully implemented. An effective training and education plan to equip NARA's stakeholders with the knowledge and information needed will not only apply risk management to their day-to-day jobs, but will help champion NARA's effort to develop a formalized risk-based ICP.

Lack of attention and commitment
When CP originally started working on the ICP there were competing priorities, including the Transformation effort, which the one staff person from CP was originally involved in along with NARA's Management Team. In order to have a successful ICP, NARA's Management Team can no longer overlook the program as more input and oversight is required. As noted in the *Business Transformation Plan* (issued May 29, 2011), NARA committed to establishing an ERM capability and a Risk Officer to analyze and manage risks and opportunities. NARA has yet to identify a Risk Officer, but in response to GAO's recommendation, in 2011 NARA established the Management Control Oversight Council (MCOC). The MCOC is comprised of all members of NARA's Management Team, with the Chief Operating Officer (COO) serving as the chair. Although the MCOC was created to provide leadership and oversight necessary for effective implementation of NARA's ICP, they have not met their purpose. Since the creation of the MCOC, the quarterly meetings solely focused on reviewing action plans for the agency's material weaknesses and risks for FMFIA reporting purposes. Based on our review of the minutes from the meetings, (1) CP is not actively involved in the meetings to discuss the ICP, (2) no new weaknesses or risks have been identified, and (3) no directives have been issued regarding implementation of the ICP.

The COO indicated Senior Management is very committed to seeing the ICP developed. He also stated he (1) sees the ICP as an opportunity for NARA managers to take ownership of problems, (2) would like to avoid the identification of material weaknesses only by the OIG, and (3) would like to see managers identify problems earlier. He is hopeful the ICP planned by CP will assist in the process. Based on the current internal control environment, the outcomes the COO would like to see from an ICP would most likely not be possible. Until Senior Management formally acknowledges and puts in place the necessary resources, the program will continue to under deliver. Additionally, absent of having an ICP, audits performed by the OIG or oversight agencies will continue to be the sole source for systematically identifying risks.

The OIG inquired with Senior Management about (1) how far along NARA was in establishing an ERM capability and (2) what was limiting an ERM capability from being implemented. Management did not provide a definitive answer or specific details as to the state of the ERM and any limitations. Additionally, the OIG inquired about identifying a Risk Officer for the agency. The COO indicated his position will now serve as the Risk Officer and NARA 101 will be updated to reflect this change. This decision does not show management's commitment to ERM or emphasize the importance of it.

Currently, there are eight offices that report to the COO position including (1) Federal Register, (2) Agency Services, (3) Research Services, (4) Information Services, (5) Business Support Services, (6) Legislative Archives, Presidential Libraries, and Museum Services, (7) Corporate Records Management, and (8) CP. According to a McKinsey & Company's report, *Strengthening Risk Management in the US Public Sector*, public sector institutions should establish a dedicated risk-management organization that resides in a prominent place in the organization. The Chief Risk Officer should either be at the same level as the COO or Chief Financial Officer (CFO), or at most one level below. It further states risk personnel should have deep knowledge of both risk management and the institution's business. NARA would benefit by selecting an individual that (1) could devote majority of their time to effectively leading the implementation and management of an ICP, (2) possesses risk management skills, and (3) possesses the capability to build a risk-aware culture agency wide.

Lack of resources
Budget resources to hire staff and develop an ICP system have not been made available to support the implementation of the ICP. Currently, only one CP employee is assigned to implement the ICP. The program is too large and complex for one person to implement the program across the agency. The COO originally indicated to the OIG no additional staffing resources were available, but since then the hiring of one additional staff member has been approved. The ICP for a similar size agency, the Library of Congress, is administered in the Library's Strategic Planning Office of the Chief Financial Officer. The Library has one ICP Administrator and 11 ICP Coordinators, which are the ICP administrators for every service unit at the Library.

According to a McKinsey & Company report, *Strengthening Risk Management in the US Public Sector*, public sector institutions should push for legislation that requires the appointment of a Chief Risk Officer (CRO) and the formation of a risk-management department, with specific details about the roles, responsibilities, and qualifications of risk-management staff. The report further stated the risk organization's structure should mirror the agency's structure, with dedicated risk personnel for each focus area. The exact size of the risk organization will vary by agency, but it must at least be large enough so that it can dedicate one or two people to each high-priority area. While the one additional resource will be beneficial to the ICP, program implementation and management will continue to be a challenge, and program benefits will be under realized, until an adequate amount of resources are employed to support the program.

CP was not given the funding to procure software and is now internally developing a Microsoft Access database to support automation of the internal control/risk management program. The database will not (1) have the capability to adequately support a robust ICP, (2) append information to support decisions about the criticality of functions, inherent and residual risks, and the results of testing and monitoring activities, (3) support automatic notification of events based on a hierarchical structure, and (4) accommodate automated alerts for significant events such as when a new function is added and the criticality of a program/function is changed by this event. New software to support the ICP (estimated to cost $200,000 initially and $12,000 annually for maintenance) would

(1) automate the reporting and sharing of information concerning functions, risks, controls and performance data across the agency and (2) allow for the assignment and tracking of risks and recommendations. In our opinion, the cost of the software is minimal in comparison to the intangible benefits that would be gained by the agency.

Performance and Accountability Office and Office of Strategy

Currently there are two different offices, CP and Division of Strategy, performing similar responsibilities as it relates to internal controls. According to NARA 101, *NARA Organization and Delegation of Authority*, CP is delegated the authority to coordinate NARA's implementation of OMB Circular A-123, the NARA internal management control review system, independent internal testing, enterprise risk management, and the Federal Managers' Financial Integrity Act. CP also serves as NARA's Risk Officer, overseeing the agency's ERM program. The Strategy Division (within the Strategy and Communications Office) is responsible for coordinating and facilitating NARA issues management and strategic policy analysis activities as well as engaging NARA staff and stakeholders to address the agency's goals, issues and opportunities.

The Strategy's Division responsibilities appear to be parallel and in direct conflict with the authority delegated to CP as they are related to the ICP. A part of administering an ICP is identifying risk, quantifying risk exposure, assigning risk ownership, determining mitigation strategy, and tracking and managing mitigation to closure. CP indicated there has been no formal coordination or sharing of information between CP and the Strategy Division regarding risks and issues management. The OIG attempted, but was unable to discuss the Strategy's Division role in identifying agency risks for the Strategic Plan and whether there was any overlap with the ICP work performed by CP. The Strategy Division cannot coordinate and facilitate issues management if it is not in communication with the office in charge of implementing the ICP. It is also not beneficial for these two offices to be working in silos and not effectively communicating.

Recommendation

The Archivist of the United States should demonstrate a commitment to the development, implementation, and operation of NARA's ICP by ensuring:

a) The MCOC becomes more involved in the decision making and implementation plan for the ICP. Additionally, periodic reports (at least quarterly) must be presented to the MCOC to review the progress of the ICP.
b) All risk management activities (identifying controls, risks, tactical risks, issues management, etc.) are coordinated with CP, who is delegated the authority of overseeing the agency's ERM program.
c) Revisions are made to the existing project plan outlining concise, detailed tasks required for full implementation of the ICP (from current status to full implementation).
d) Resources are employed to develop and implement the ICP, including but not limited to a Chief Risk Officer, additional employees or contractors, and the purchase of appropriate ICP software.
e) Risk management responsibilities are included in the performance plans for program and function owners.
f) Prior recommendations from previous OIG and GAO reports are closed.
g) A Risk Management Policy is created to communicate NARA's commitment to enterprise risk management.
h) Procedures are documented that clearly document the ICP, including outlining a process for tracking issues and corrective actions identified.
i) A training plan is developed that encompasses educating the agency on risks and internal control. Additionally, training is provided to all individuals responsible for executing the ICP, including program owners, function owners, and MCOC members.

Management Response

Management concurred with the recommendation.

Appendix A – Status of Prior Recommendations

The chart below identifies audit recommendations from prior OIG and GAO reports regarding NARA's Internal Control Program.

Recommendation[7]	Status
Director of Policy and Planning should work with offices in general, and management control liaisons in particular, to: (1) stress the importance of performing internal control assessments of critical areas in accordance with management control plans and NARA 114; (2) ensure the results of the assessments are included in the assurance statements, and; (3) revise, as necessary, the lists of "critical functions" to be reviewed. (OIG 09-14)	Partially implemented (only item 3 is implemented)
Assistant Archivist for Administrative Services should ensure Annual Information Security Self Inspection results are reviewed in a timely manner, instances of non-compliance are identified, and corrective actions are monitored; and self inspections are reviewed and documented in accordance with guidance concerning self-assessments contained in NARA 114. If a formal process as referred to by the Information Security Officer cannot be completed in time to facilitate the review of FY 2009 information security self inspections an alternate means of reviewing the checklists should be developed. (OIG 09-14)	Implemented
AOTUS should ensure NARA policy on internal controls (such as NARA 114) is revised to specifically address the process by which findings are evaluated and categorized; criteria used in the decision making process, and; documentation necessary to support such conclusions. (OIG 09-14)	Not implemented
Assistant Archivist for Regional Records Services should ensure all program findings, regardless of whether they are considered major or minor, are tracked to resolution and supported by adequate documentation. (OIG 09-14)	Not implemented
AOTUS should demonstrate a commitment to the internal control program by establishing centralized responsibility within NARA's existing organizational structure or within the proposed Performance & Accountability Office (as indicated in the Proposed NARA Organization Report from the Archivist's Task Force on Agency Transformation). (OIG 10-19)	Implemented
AOTUS should formalize the Internal Control program to include the five standards for internal control: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. (OIG 10-19)	Not implemented
AOTUS should consider establishing a Senior Management Council to provide oversight and additional accountability for the Internal Control Program. (OIG 10-19)	Implemented
AOTUS should ensure that NARA's senior staff and decision makers can appropriately and quickly assess threats and vulnerabilities stemming from enterprise risks, develop and assign responsibility and resources for an enterprisewide risk management capability that allows it to monitor its internal and external environments continuously and systematically. (GAO-11-15)	Not implemented

---

[7] After the Transformation effort in 2011, office names and symbols subsequently changed to reflect the current reorganization. However, the previous office names are used in the chart above to reflect the historical names of the offices recommendations were addressed to in previous audit reports.

Appendix B – Acronyms and Abbreviations

AOTUS	Archivist of the United States
COO	Chief Operating Officer
CFO	Chief Financial Officer
CP	Performance and Accountability Office
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
FMFIA	Federal Managers' Financial Integrity Act
GAO	Government Accountability Office
ICP	Internal Control Program
MCOC	Management Control Oversight Council
NARA	National Archives and Records Administration
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAR	Performance and Accountability Report
Circular A-123	Circular A-123, Management's Responsibility for Internal Control
WNRC	Washington National Records Center

Appendix C – Management's Response to the Report

NATIONAL ARCHIVES

Date: NOV 1 9 2012

To: James Springs, Acting Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: OIG Revised Draft Audit 13-01, Audit of NARA's Internal Control Program

Thank you for the opportunity to provide comments on this draft report. We appreciate your willingness to revise some language in the original report.

We concur with the nine recommendations in this audit, one of which is an accumulation of four recommendations from previous audits that have not been implemented as well as one that has been only partially implemented.

We have one additional comment related to the last paragraph under "Lack of Attention and Commitment" (Pgs. 11-12) – We recognize there are several places within an organization where a risk officer may reside and we have, at this time, identified CP as the office responsible for carrying out risk management activities with the COO serving as Chief Risk Officer. As our program matures, we will return to your observation about CRO placement for consideration.

If you have any questions or need additional information on these comments, please contact Mary Drak by phone at 301-837-1668 or via email at mary.drak@nara.gov.

David S. Ferriero
Archivist of the United States

NATIONAL ARCHIVES and
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix D – Report Distribution List

Archivist of the United States (N)
Deputy Archivist of the United States (ND)
Chief Operating Officer (C)
Executive of Agency Services (A)
Chief Financial Officer (BC)
Director, Performance and Accountability (CP)
Management Control Liaison, Performance and Accountability (CP)