



OFFICE of INSPECTOR GENERAL  
NATIONAL ARCHIVES and RECORDS ADMINISTRATION  
8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001  
[www.archives.gov/oig](http://www.archives.gov/oig)

October 28, 2016

**TO:** David S. Ferriero  
Archivist of the United States

**FROM:** James Springs *James Springs*  
Inspector General

**SUBJECT:** *Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls-Audit Report No. 17-AUD-01*

Attached for your action is Cotton & Company's final report, *Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls*. Cotton & Company incorporated the formal comments provided by your office.

In connection with the contract, we reviewed Cotton & Company's report and related documentation and inquired of its representatives. Cotton & Company is responsible for the attached auditor's report dated October 28, 2016, and the conclusions expressed in the report. However, our review disclosed no instances where Cotton & Company did not comply, in all material respects, with Generally Accepted Government Auditing Standards.

The report contains eight recommendations aimed at strengthening NARA's internal control environment. Your office concurred with the recommendations. Based on your October 26, 2016 response to the draft report, we consider all the recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed upon corrective actions so that recommendations may then be closed.

As with all OIG products, we will determine what information is publicly posted on our website from the attached report. Should you or management have any redaction suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Consistent with our responsibility under the *Inspector General Act, as amended*, we may provide copies of our report to congressional committees with oversight responsibility over the National Archives and Records Administration.

Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.

Report No. 17-AUD-01

**Cotton & Company's**  
**Enterprise-Wide Risk Assessment Audit of**  
**NARA's Internal Controls**

**October 28, 2016**



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

James Springs  
Inspector General  
National Archives and Records Administration  
8601 Adelphi Rd, Room 1300  
College Park, MD 20740

Subject: Enterprise-Wide Risk Assessment Services to the National Archives and Records Administration

Cotton & Company LLP is pleased to submit this independent report on the National Archives and Records Administration (NARA)'s enterprise-wide risk assessment of internal controls and the risks to NARA's mission, operations, and procedures. We conducted this performance audit in accordance with the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We carried out testing during the period from October 1, 2015, through July 8, 2016.

Sincerely,

COTTON & COMPANY LLP

A handwritten signature in cursive script that reads "George E. Bills".

George E. Bills, CPA, CISSP, CISA, CIPP  
Partner, Information Assurance

October 28, 2016  
Alexandria, Virginia

# Table of Contents

---

<b>Executive Summary</b> .....	1
<b>Objectives, Scope, and Methodology</b> .....	4
<b>Audit Results</b> .....	6
<i>1. NARA Has Not Fully Implemented an ERM Program</i> .....	6
<i>Recommendations:</i> .....	7
<i>2. NARA’s Internal Control Program Needs Improvement</i> .....	7
<i>Recommendations:</i> .....	10
<i>3. NARA’s Privacy Controls Need Strengthening</i> .....	11
<i>Recommendations:</i> .....	12
<i>4. Top 17 NARA Challenges</i> .....	13
<b>Table 1 Top 17 NARA Challenges</b> .....	13
<i>5. Issues With NARA’s Control Environment</i> .....	17
<b>Table 2 Known Weaknesses</b> .....	17
<i>Suggestions:</i> .....	20
<b>Appendix A – Acronyms and Abbreviations</b> .....	21
<b>Appendix B – Management’s Response to the Report</b> .....	22
<b>Appendix C – Report Distribution List</b> .....	25

# Executive Summary

---

The National Archives and Records Administration (NARA), Office of Inspector General (OIG) engaged Cotton & Company LLP to perform an enterprise-wide risk assessment of NARA's internal controls and the risks to its operations and procedures, in accordance with Generally Accepted Government Auditing Standards. The Federal Managers' Financial Integrity Act (FMFIA) and Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, provide guidance for implementing an internal control program (ICP). This guidance requires agency heads to conduct ongoing internal control reviews and to evaluate and report annually on their systems of internal accounting and administrative control.

The purpose of this audit was to perform an enterprise-wide risk assessment of NARA's internal controls and the risks to NARA's operations and procedures. We conducted our testing from October 1, 2015 to July 8, 2016. Results from our testing are noted below.

While NARA appears to be aware of the significant risks and challenges they face, NARA has yet to implement an enterprise-wide risk management (ERM) program that clearly identifies, prioritizes, and manages risks throughout the organization. NARA management has not made the implementation of an ERM program a strategic priority and instead has been relying on their ICP and Management Control Oversight Council to identify and manage risks throughout the organization. As a result, management's internal control activities and assurance statements continue to be based on work at the individual function, program, and office level. This stove-piped focus does not result in risks that span across the enterprise, such as those related to information security, hiring, and the allocation of limited resources, being evaluated by all affected offices, programs, and functions to ensure risks within each office are at an acceptable level. Additionally, without an effective ERM process in place that clearly identifies, categorizes, and assesses the effectiveness of controls related to key risks, the Archivist's annual assurance statement to the President and Congress may not clearly reflect NARA's current internal control environment, including risks.

In addition, while NARA implemented an ICP, we noted its implementation of the program needs improvement. Requirements outlined in NARA's existing policies and procedures were not consistently followed by the offices and programs responsible for completing ICP activities. Additionally, NARA's lack of a fully implemented ERM program means risks identified during the ICP process are not formally aligned to NARA's strategic goals and objectives. This occurred primarily due to a lack of formal training and oversight of ICP activities being carried out. NARA's weaknesses with its ICP mean it is not realizing important benefits of an effective ICP that include:

1. Improved decision-making
2. Improved risk identification, management, and mitigation
3. Opportunities for process improvement

4. Effective use of budgeted resources
5. Improved strategic planning

In addition, during the audit we identified 17 challenges<sup>1</sup> we believe present the greatest risk to NARA's operations and its ability to achieve its stated strategic goals and mission.

This report makes eight recommendations which we believe, once implemented, will strengthen NARA's internal control environment and provide senior management with greater assurance that management's conclusions in their formal assurance statements are accurate. We also provide management with five suggestions that, if implemented, should help management improve their controls over high risk areas within the organization.

---

<sup>1</sup> These 17 challenges are based on auditor judgement and were identified as a result of reviewing NARA documentation and conducting interviews with NARA personnel. Each of these challenges has risks associated with it that, if realized, could negatively impact NARA's ability to carry out its mission.

## 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, agency heads must annually evaluate and report on their systems of internal accounting and administrative control by preparing and delivering to the President and Congress, an annual assurance statement.

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 and the process for assessing internal control effectiveness 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. The internal control standards and the definition of internal control used in Circular A-123 are based on the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*.

GAO *Standards for Internal Control in the Federal Government* define internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. To meet those objectives, management is responsible for developing and maintaining internal control activities that comply with the following internal control standards: (1) Control Environment; (2) Risk Assessment; (3) Control Activities; (4) Information and Communications; and (5) Monitoring.

On February 25, 2014, NARA issued NARA 160, *Enterprise Governance, Risk and Compliance Program*, replacing NARA 114, *Management Controls* which had established policy for improving accountability and effectiveness of NARA programs and operations by establishing, assessing, correcting, and reporting on management controls. NARA 160 describes the structure, roles and responsibilities of NARA's EGRC including the Archivist's responsibility to provide ultimate assurance to the President and Congress on the effectiveness of NARA internal accounting and administrative controls. Additionally, NARA 160 describes the three major components that make up NARA's EGRC program: (1) NARA 161, *Internal Control Program (ICP)*; (2) NARA 162, *Enterprise Risk Management (ERM)*; and (3) NARA 163, *Issues Management*. As of July 8, 2016, only NARA 161 had been developed and implemented.

## Objectives, Scope, and Methodology

---

The objective of this audit was to perform an enterprise-wide risk assessment of controls and the risks to NARA's operations and procedures. Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as established in the Government Accountability Office (GAO)'s *Government Auditing Standards*, December 2011 Revision. To achieve the above objective, we met with various personnel from offices throughout NARA, including:

- Chief Operating Officer
- Chief Records Officer
- Office of Strategy and Communications
- Office of Human Capital
- Office of Innovation
- Federal Register
- Agency Services
- Research Services
- Legislative Archives, Presidential Libraries, and Museum Services
- Information Services
- Business Support Services
- General Counsel
- Accountability Staff

During these meetings, we obtained an understanding of the office's major activities and how those activities support NARA's mission and strategic goals. We identified challenges that each office faces in meeting its day-to-day responsibilities and the risks those challenges present to NARA. In addition, we obtained and reviewed relevant NARA, GAO, and OIG documentation and reports to strengthen our understanding of NARA's core activities and challenges, as well as to determine where issues with NARA's internal controls had already been identified. Documents reviewed ranged from NARA's strategic goals and performance plans to the OIG's semiannual reports to Congress and existing assessments of NARA's ICP.

To evaluate NARA's ERM program and the effectiveness of key internal controls, we conducted a series of interviews with the Chief Operating Officer (COO), ICP administrator, and Office of Strategy and Communications and reviewed ICP reports and supporting documentation submitted by various NARA offices to gain an understanding of how each office carried out ICP requirements.



In addition, during our audit we identified the following 17 challenges<sup>2</sup> that we believe present the greatest risk to NARA's operations and its ability to achieve its stated strategic goals and mission.

1. Effectiveness of NARA's ERM Program
2. Lack of Adequate Funding
3. Availability of Physical Storage Space
4. Hiring Challenges
5. Effectiveness of NARA's Information Security Management Program
6. Safeguarding of Classified Information
7. Safeguarding of Sensitive Personally Identifiable Information (PII)
8. Effectiveness of Physical Holdings Security (Holdings Protection Program)
9. Effectiveness of NARA's Digitization Effort
10. Quality and Timeliness of National Personnel Records Center (NPRC) Services
11. Effectiveness of NARA's Records Management Activities
12. Effectiveness of NARA's Processing Program Activities
13. Effectiveness of NARA's Preservation Activities
14. Lack of Sufficient Electronic Data Storage
15. Effectiveness of NARA's Project Management Activities
16. Timeliness of Contract Management
17. Ability to Operate During a Government Shutdown

For each of these challenges, we conducted interviews with NARA personnel and reviewed NARA's ICP documentation to determine whether risks and controls related to our 17 challenges had been formally identified in NARA's ICP and related controls evaluated for effectiveness. Where controls were identified, we performed independent testing to determine if those controls were in place and operating effectively. Specifically, we:

- Conducted interviews with NARA personnel and obtained and reviewed ICP documentation, directives, policies, and procedures to identify key controls that management had in place.
- Reviewed NARA OIG and GAO reports, including the OIG FY 2016 Semiannual Open Recommendation Report, to determine if key controls had already been tested and determined to be ineffective.
- Conducted interviews, and obtained and reviewed supporting documentation to verify that key controls were in place and operating effectively.

This report is intended solely for the information and use of the NARA OIG and management, and is not intended to be and should not be used by anyone other than these specified parties.

---

<sup>2</sup> These 17 challenges are based on auditor judgement and were identified as a result of reviewing NARA documentation and conducting interviews with NARA personnel. Each of these challenges has risks associated with it that, if realized, could negatively impact NARA's ability to carry out its mission.

# Audit Results

---

## *1. NARA Has Not Fully Implemented an ERM Program*

While NARA appears to be aware of the significant risks and challenges they face, NARA has yet to fully implement an ERM program that clearly identifies, prioritizes, and manages risks throughout the organization. We noted NARA management has not made the implementation of an ERM program a strategic priority and instead has been relying on its ICP and Management Control Oversight Council to identify and manage risks throughout the organization. As a result, NARA's internal control activities and assurance statements continue to be based on work at the individual function, program, and office level. This stove-piped focus does not result in risks that span across the enterprise, such as those related to information security, hiring, and the allocation of limited resources, being evaluated by all affected offices, programs, and functions to ensure risks within each office are at an acceptable level. Without an effective ERM process in place that clearly identifies, categorizes, and assesses the effectiveness of controls related to key risks, the Archivist's annual assurance statement to the President and Congress may not clearly reflect NARA's current internal control environment, including risks.

In 2014, NARA developed and documented NARA 160, *Enterprise Governance Risk and Compliance* which put in place an overarching policy and framework for the implementation of an ERM program. NARA 160 is comprised of three major components that include: (1) NARA 161, *NARA's Internal Control Program*; (2) NARA 162, *NARA's Enterprise Risk Management Program*; and (3) NARA 163, *NARA's Issues Management Program*. Of the three components, NARA had only developed, documented, and implemented the ICP.

NARA 160 states: "*The capabilities inherent in enterprise risk management help management achieve performance and financial targets and prevent loss of resources. Enterprise risk management ensures effective reporting related to NARA's mission accomplishment while complying with laws and regulations.*" Further, NARA 160 section 160.6, *What are the benefits of an EGRC program* states: "*Some potential benefits from instituting a more robust, repeatable, and coherent EGRC program include, but are not limited to:*

- a. Identification of a single set of agency wide functions from a business perspective;*
- b. Identification of the relative importance of functions;*
- c. Alignment of risks, opportunities, controls, and measures to functions;*
- d. Better alignment of focus and resources based on importance of function and risk;*
- e. Improved ability to make and defend decisions about resource allocations, risk management approaches, and the level of internal controls associated with functions;*

- f. *Improved information sharing, analysis, and decision making;*
- g. *Improved ability to analyze, track and resolve audit recommendations;*
- h. *Strengthening NARA's internal control and risk management programs by addressing and closing existing OIG and GAO recommendations; and*
- i. *Improved ability to anticipate and manage expectations of stakeholders through issues management."*

While NARA 160 clearly acknowledges many of the benefits of implementing an ERM program, NARA management has not made the implementation of NARA 162 and 163 a priority. At the time of our testing, management did not have a plan including target completion dates for the implementation of NARA 162 and 163.

***Recommendations:***

We recommend that the Chief Operating Officer \ Chief Risk Officer:

1. Fully implement all components of NARA 160, including:
  - a. Developing, documenting, and fully implementing NARA 162, *NARA's Enterprise Risk Management Program*. Within NARA 162, roles and responsibilities for ERM activities should be clearly identified.
  - b. Developing, documenting, and fully implementing NARA 163, *NARA's Issues Management*.
2. Develop, document, and implement a formal process to:
  - a. Identify and prioritize risks within the organization. Risks should be tied directly to NARA's strategic plan and mission and prioritized based on their overall importance to the agency.
  - b. Prioritize risk management activities including the use of limited resources based on key risks within the organization. Management's prioritization should be clearly documented and include formal steps to ensure risks are maintained at an appropriate level.

***2. NARA's Internal Control Program Needs Improvement***

While NARA has implemented an ICP, we noted its implementation of the program needs improvement. Specifically, requirements outlined in NARA's existing ICP policies and procedures were not consistently followed by the offices and programs responsible for completing ICP activities. Additionally, NARA's lack of an ERM program means risks identified during the ICP process are not formally aligned to NARA's strategic goals and objectives. This occurred primarily due to a lack of formal training and oversight of all ICP activities being carried out NARA offices and programs. NARA's

weaknesses with its ICP mean it is not realizing important benefits of an effective ICP that include:

1. Improved decision-making
2. Improved risk identification, management, and mitigation
3. Opportunities for process improvement
4. Effective use of budgeted resources
5. Improved strategic planning

We noted a number of instances where required ICP documentation was not submitted, submissions were incomplete, or did not include adequate detail to support conclusions made. While the ICP administrator did provide assistance to NARA personnel during the ICP process, we noted this did not include reviewing submissions for compliance with NARA's ICP policy and following up where non-compliance was identified to obtain updated or corrected documentation. Further, we noted formal ICP training had not been developed and provided to individuals responsible for ICP activities to ensure they had a clear understanding of the ICP process and its requirements.

In December of 2012, the OIG issued Audit Report No. 13-01 *Audit of NARA's Internal Control Program*, which included one finding titled *NARA has yet to establish an Internal Control Program*. In this report, the OIG noted that "*Although Senior Management agreed to formalize NARA's ICP in 2010, the program has yet to be developed and fully implemented.*"

Since the issuance of the OIG's 2012 audit report, NARA developed and implemented NARA 161, *NARA's Internal Control Program*. NARA 161 states the Chief Operating Officer (COO) who is also the Chief Risk Officer (CRO), is responsible for affirming with reasonable confidence, through the Annual Statement of Assurance to the Archivist, that internal controls are in place and operational. These assurance statements are based on results of internal control monitoring, testing and reporting conducted by NARA offices, via NARA's ICP; information obtained and evaluated by management through daily operations; discussions of weaknesses and risks conducted by NARA's internal control and risk management body and; audits and evaluations conducted by NARA's OIG, the GAO, and other third parties.

In addition, NARA 161 assigns staff within Accountability (CA, formerly Performance and Accountability - CP) as the administrator of NARA's ICP and defines their role as assisting managers in developing internal controls for each function for which they are responsible for. While NARA 161 provides detailed information on the structure, roles and responsibilities of NARA's ICP, we noted management's implementation of the ICP is not effective.

#### Required Documentation Not Submitted

We reviewed FY 2015 ICP submissions for each of the NARA's 12 offices and identified a number of instances where required documentation was not submitted. Specifically, we

noted two offices did not submit risk assessment reports. NARA 161, Appendix A, *Internal Control Program Guidance*, requires all offices to submit risk assessment reports that identify the functions selected for testing in the coming fiscal year. Of the ten offices that did submit risk assessment reports, three did not provide their rationale for classifying functions as high risk or high criticality as required by NARA's *Instructions for Identifying High Risk or Critical Functions*.

In addition, we noted five NARA offices' ICP submissions did not include monitoring plans for all functions. NARA 161, Appendix A, *Internal Control Program Guidance*, requires all offices' ICP submissions to report on the controls that are in place to monitor all functions and to document the methods used to monitor controls. We also noted four of the offices' ICP submissions did not include monitoring results for all functions. NARA 161, Appendix A, *Internal Control Program Guidance*, requires all offices' ICP submissions to report on the controls that are in place to monitor all functions and to document the results of this monitoring.

Additionally, the ICP submission for one of the 12 offices did not contain test plans for all high-risk or highly critical functions. NARA 161, Appendix A, *Internal Control Program Guidance*, requires offices to test functions identified as either high risk or highly critical and to include test plans, including the test methodology and test results, in the ICP submission. Finally, two offices' ICP submissions did not include test results for all high-risk or highly critical functions. NARA 161, Appendix A, *Internal Control Program Guidance*, requires offices to test functions identified as either high risk or highly critical and to include test plans, including the test methodology and test results, in the ICP submission.

While CA is responsible for administering NARA's internal control program and does interact regularly with NARA offices and programs, we noted CA does not perform comprehensive reviews of management's ICP submissions to ensure they comply with all ICP requirements outlined in NARA 161. As the OIG noted in its 2012 audit of NARA's Internal Control Program, "*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.*" While NARA has added an additional resource to CA since the 2012 audit, we noted inadequate resources were repeatedly communicated to us as a key factor limiting CA's ability to fully implement and manage the ICP process.

#### Quality and Completeness of ICP Documentation

In addition to required documentation not being submitted, our review of NARA's FY2015 ICP submissions noted significant differences in the quality and completeness of ICP documentation submitted. Depending on the program or function owner, test plans varied from providing clear steps and evidence demonstrating the specific actions that the office would take to test the function, to only identifying the areas to be tested without detailing any test steps or actions.

We noted a number of test plans for high rated functions were put on hold or not completed during FY2015 to support management's statements of assurance. In some cases, multiple offices and their functions used their monitoring plans as their test plans. NARA's ICP Guideline differentiates between the two plans. In addition, we noted test plans for several functions did not include steps to test risks identified but rather described the function's process. Further, a number of test plans and results of testing reviewed provided insufficient narratives and did not provide clear explanations on what was tested and how it was tested.

Finally, in other instances, offices were inconsistent with regard to the content and quality of their reported test results. Depending on the program or function owner, test results varied from providing clear summaries of the office's testing methodology, findings, corrective action plans, and results of each step taken, to providing only a final conclusion that states that the office completed the testing, with no supporting evidence. NARA 161, Appendix A, *Internal Control Program Guidance*, states that offices' ICP submissions must include their detailed test methodology and a summary of testing results, including findings, corrective actions, and a reference indicating where the reader can obtain the full testing results.

***Recommendations:***

We recommend that the Chief Operating Officer \ Chief Risk Officer:

3. Provide additional resources to the Office of Accountability to ensure ICP activities are effectively carried out.
4. Develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review:
  - a. To ensure all required documentation has been submitted by the due date. Where documentation has not been provided, NARA should have a formal process in place to follow up and obtain the required documentation.
  - b. Of ICP documentation submitted to ensure it is both complete and accurate. Where discrepancies are identified, NARA should have a formal process in place to follow up with management so corrections can be made.
  - c. Of each office's submission to determine whether risks identified and conclusions made are appropriately supported.
  - d. Of test plans and test results for all high-risk or highly critical functions to ensure they clearly demonstrate the office's methodology for performing testing and reaching conclusions.

- e. Of monitoring plans and monitoring results for all functions that clearly show the extent of monitoring performed, the office's methodology for performing the monitoring, and the rationale for its conclusions.
5. Develop and fully implement a formal ICP training program. NARA's ICP training program should identify and require individuals who are involved with NARA's ICP to complete initial training and refresher training periodically thereafter. Further, management should track completion of ICP training to ensure all individuals involved in the ICP process have received adequate training.

### ***3. NARA's Privacy Controls Need Strengthening***

While NARA has policies and procedures in place that outline how to handle and secure privacy data, we noted NARA does not periodically evaluate the effectiveness of its privacy policies and procedures. While NARA General Counsel's (NGC) FY2015 assurance statement does address privacy by noting "*As the senior Agency Official for Privacy, I am responsible for the oversight of NARA's privacy policies, including the protection of PII. I work closely with the Privacy Act Officer, the Assistant General Counsel for privacy issues, the Chief Information Officer (I), and the Chief Information Security Officer (IT) in developing and implementing policy in response to OMB directives and other requirements. I also am a member of the NARA Privacy Breach Response Team,*" we noted this statement focuses largely on the development and implementation of the privacy policy and not on the effectiveness of controls over sensitive PII.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control AR-4 *PRIVACY MONITORING AND AUDITING* states. "*The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.*" NARA management did state that it is in the process of hiring an individual whose responsibilities would include conducting periodic assessments of privacy controls.

#### Privacy Rules of Behavior

We also noted NARA does not require employees, contractors, and other individuals that may handle or come into contact with sensitive PII to sign its privacy rules of behavior. While NARA's annual security awareness training mentions the privacy rules of behavior, individuals are not required to fully read and sign these rules as part of that training. We determined NARA does not require personnel to sign the privacy rules of behavior because management does not believe that it would provide substantial value. While requiring individuals to sign formal rules of behavior may not significantly strengthen existing controls, without requiring personnel to read and formally sign privacy rules of behavior, management has less assurance that personnel are aware of and are following required privacy practices. In addition, requiring individuals to formally

sign the rules of behavior strengthens management's ability to hold individuals accountable when they violate these rules.

NIST SP 800-53, Revision 4, control *PL-4 RULES OF BEHAVIOR* states, "*The organization: b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.*"

### PII System Inventory

Finally, while NGC emails system owners to request verification that the systems have not undergone any changes that require NARA to update the system's privacy impact assessment (PIA), NGC does not have controls in place to verify that it receives responses from all individuals. We inquired with NGC management and found that it does not always follow up on all PII update inquiries because it is generally aware of system changes that would require updates to the privacy inventory (e.g., PIAs and Systems of Records) due to its involvement in NARA's Investment Review Board. NGC management therefore may not follow up on an outstanding inquiry if it believes that it already knows the answer. Not requiring responses for all emails regarding PII updates increases the risk that changes to NARA's environment will occur without management's knowledge and that management therefore will not put appropriate controls in place over sensitive PII.

In addition, NIST SP 800-53, Revision 4, control *DM-1 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION* states, "*The organization: c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.*"

Without an effective ICP in place to identify privacy risks and periodically assess controls, management's assurance that internal controls are in place and operating as intended is not fully supported.

### ***Recommendations:***

We recommend that the NARA General Counsel:

6. Develop, document, and fully implement policies and procedures to ensure NARA personnel (i.e., employees, contractors, and others with access to NARA systems or information) review and formally acknowledge their responsibilities to comply with NARA's privacy rules of behavior annually.
7. Implement a process for following up on outstanding system change inquiries and obtaining the requested information.



8. Develop, document, and implement policies and procedures to periodically test the effectiveness of privacy policies, procedures, and controls.

#### **4. Top 17 NARA Challenges**

Through our interviews with NARA personnel and review of key documents, including NARA’s Strategic Plan, directives, FY2015 assurance statements, ICP documentation and OIG and GAO audit reports, we identified 17 challenges<sup>3</sup> that we believe present the greatest risk to NARA’s operations and its ability to achieve its stated strategic goals and mission. For each of these challenges, we identified related risks and controls so that we could evaluate the effectiveness of NARA’s overall internal controls environment. The top 17 challenges we identified during our audit are noted below.

**Table 1 Top 17 NARA Challenges**

<b>No.</b>	<b>Challenges</b>	<b>Description</b>
<b>1</b>	Effectiveness of NARA’s ERM Program	An effective ERM program ensures that the agency identifies key risks and uses its limited resources in the most efficient and effective manner possible. Without an effective ERM program in place, management may be subject to higher levels of risk than they would otherwise accept. See further discussion on NARA’s ERM in the audit results section.
<b>2</b>	Lack of Adequate Funding	Various NARA personnel and offices noted that they had insufficient funding to carry out their required duties. While NARA’s holdings and required activities continue to grow, NARA’s funding does not appear to be keeping pace with this growth. In addition, some individuals noted funding decisions are not transparent or understood by everyone in the organization. Without adequate funding, many of NARA’s highly critical functions are at significantly greater risk of failing.
<b>3</b>	Availability of Appropriate Physical Storage Space	NARA has currently filled 88 percent of its available physical space. Challenges to acquiring additional physical storage space include both the cost of the space and the physical and environmental requirements that NARA must meet. Without additional space, NARA may not be able to accept new records or holdings or adequately safeguard holdings currently in their possession.

<sup>3</sup> These 17 challenges are based on auditor judgement and were identified as a result of reviewing NARA documentation and conducting interviews with NARA personnel. Each of these challenges has risks associated with it that, if realized, could negatively impact NARA’s ability to carry out its mission.

<b>No.</b>	<b>Challenges</b>	<b>Description</b>
4	Hiring Challenges	Multiple offices identified NARA's inability to properly staff existing and future positions as a significant risk to their ability to complete their missions. This issue included not only an overall lack of staff members, but also a lack of staff members with the right skill set. Without both adequate and appropriate staff, NARA may be unable to effectively carry out its day-to-day activities.
5	Effectiveness of NARA's Information Security Management Program	NARA continues to have a significant number of weaknesses related to IT. We noted that the OIG and NARA management have identified IT security as a material weakness. While IT security is a significant challenge for all federal agencies, without effective IS controls in place, NARA's systems and data are at greater risk of unauthorized access or disclosure.
6	Safeguarding of Classified Information	NARA collects and maintains classified data for outside agencies, and proper handling and safeguarding of this data is critical. NARA must adequately protect classified data in all forms from unauthorized or accidental release; inadvertent or unauthorized leakage of such data could have a substantial negative impact, both on national security and on NARA's reputation.
7	Safeguarding of Sensitive Personally Identifiable Information	NARA handles a significant amount of sensitive PII data and faces considerable challenges in identifying when it receives this data from outside organizations, obtaining an understanding of where the data resides within NARA, and adequately protecting the data from unauthorized or accidental release. Unauthorized access or release of sensitive PII could have a substantial negative impact to the individuals whose PII is released as well as NARA's reputation.
8	Effectiveness of NARA's Physical Holdings Security (Holdings Protection Program)	NARA has been subjected to a number of thefts of physical holdings. As many of NARA's physical holdings have significant value or historical importance, it is critical that the agency has strong physical security controls in place. NARA has implemented a Holdings Protection Team, which has improved security; however, NARA's physical holdings security remains a material weakness due to inadequate oversight. Without effective physical holdings security controls in place, there is a risk that thefts of physical holdings may occur in the future.

<b>No.</b>	<b>Challenges</b>	<b>Description</b>
<b>9</b>	Effectiveness of NARA's Digitization Effort	Multiple offices identified digitization challenges as a significant issue. Digitization lacks automation, a consistent process, and proper funding; as a result, NARA is unable to ensure that it accomplishes one of its strategic goals, <i>Make Access Happen</i> . Without effective policy and procedures in place over digitization, NARA's digitization and public access goals may not be realized. In addition, records may be ineffectively digitized or stored.
<b>10</b>	Quality and Timeliness of NPRC Services	NPRC has had customer service challenges in the past, including calls that did not properly go through. Poor customer service, especially when serving current and former service members, can introduce significant reputational risk to the organization.
<b>11</b>	Effectiveness of NARA's Records Management Activities	Records management is a critical function in enabling NARA to accomplish its mission. NARA must ensure that electronic and textual records are appropriately preserved, received, referenced, delivered, and accessioned.  NARA faces continuing challenges in managing electronic records as it moves toward replacing paper records with electronic records. Without appropriate records management, NARA will be unable to meet its core objectives. We also noted that the OIG has identified electronic records management as a material weakness.
<b>12</b>	Effectiveness of NARA's Processing Program Activities	NARA personnel identified processing as a significant risk to the organization. Without adequate processing, NARA will continue to increase its backlog and will be unable to provide increased access to its customers, including online access to records. We noted that the OIG has identified NARA's processing program as a material weakness.
<b>13</b>	Effectiveness of NARA's Preservation Activities	One of NARA's fundamental objectives is to continually preserve records for the country. NARA cannot provide public access to records if it cannot properly preserve them. These preservation challenges are further increased by the constant growth of records. We noted that the OIG has identified record preservation needs as a material weakness.

<b>No.</b>	<b>Challenges</b>	<b>Description</b>
<b>14</b>	Lack of Sufficient Electronic Data Storage	Several offices identified electronic data storage as a significant risk to the organization. As NARA moves toward offering more electronic records to increase public access, it must ensure that it has sufficient storage space to achieve its strategic goal of <i>Make Access Happen</i> . Without adequate electronic storage space, records may not be collected or digitized in a timely manner. In addition, existing electronic records may be at greater risk of being lost or destroyed.
<b>15</b>	Effectiveness of Project Management	<p>With NARA's limited resources and growing responsibilities, effective project management has become increasingly important.</p> <p>NARA currently has a number of significant initiatives underway that directly impact its ability to meet its strategic goals and agency mission. Weak controls over both the monitoring and carrying out of these projects greatly increases the likelihood that they will either fail or require additional funding and resources to complete.</p> <p>Offices identified project management challenges in areas such as the implementation of the Electronic Records Archives (ERA) system and NARA's digitization projects.</p>
<b>16</b>	Timeliness of Contract Management	A number of offices stated that the length of time required to complete the acquisition process created challenges for the organization. In addition, the offices did not always effectively perform contract monitoring; this creates difficulties for NARA in working effectively with its contractors.
<b>17</b>	Ability to Operate in the Event of a Government Shutdown	NARA must prepare a plan of action for potential government shutdowns, closures, or fiscal constraints. Without advance preparation, NARA cannot ensure that it will take proper actions when these events occur. A number of NARA's activities, including Federal Register activities, must continue even when the government is closed.

## 5. Issues With NARA's Control Environment

In addition to our evaluation of NARA's ERM and ICP, we evaluated the effectiveness of key controls and processes within NARA's environment. Overall, we noted NARA has a significant number of known vulnerabilities in a number of areas throughout the organization. The majority of NARA's known vulnerabilities appear to have been identified primarily through OIG, GAO, or independent auditor reports rather than through NARA's ICP process. We discuss these vulnerabilities below.

### Significant Known Weaknesses

We noted over 280 outstanding recommendations are identified in the OIG's FY2016a Semiannual Open Recommendations report. Our review of this report noted open recommendations related to 15 of the 17 challenges we identified. We did not note any open recommendations related to NARA's ability to handle a Government Shutdown or NARA's hiring challenges. Where weaknesses related to our top 17 challenges have already been identified and are currently open, we did not perform additional testing or make further recommendations to management.<sup>4</sup>

**Table 2 Known Weaknesses**

<b>No.</b>	<b>Challenges</b>	<b>Open Recommendations Related to the Challenges</b>
1	Effectiveness of NARA's ERM Program	5
2	Lack of Adequate Funding	1
3	Availability of Appropriate Physical Storage Space	9
4	Effectiveness of NARA's Information Security Management Program	110
5	Safeguarding of Classified Information	10
6	Safeguarding of Sensitive Personally Identifiable Information	2
7	Effectiveness of NARA's Physical Holdings Security	22
8	Effectiveness of NARA's Digitization Efforts	20
9	Quality and Timeliness of NPRC Services	7
10	Effectiveness of NARA's Records Management Activities	8
11	Effectiveness of NARA's Processing Program Activities	10

<sup>4</sup> Numbers of recommendations identified related to our Top 17 challenges do not include all open OIG recommendations. In addition, some open recommendations could relate to more than one of our Top 17 challenges. As a result, the total number of open recommendations reflected in Table 2 do not equal the 280 outstanding recommendations identified in the OIG's FY 2016a Semiannual Report.

No.	Challenges	Open Recommendations Related to the Challenges
12	Effectiveness of NARA’s Preservation Activities	12
13	Lack of Sufficient Electronic Data Storage	10
14	Effectiveness of NARA Project Management Activities	10
15	Timeliness of Contract Management Activities	6

NPRC Monitoring

We noted that NPRC policies and procedures do not require management to formally document and track meeting results and issues identified. Without a formal process in place to document and track issues with NPRC’s performance, these issues may not be corrected in a timely manner.

NPRC management has a formal process in place to monitor the quality of services provided to its customers; however, we noted NPRC does not formally track issues identified and the corrective actions taken. Tracking this information would help ensure that it is correcting issues in a timely manner and would provide management with valuable lessons-learned information that could help identify organization-wide issues.

In addition, NPRC does not document the results of weekly meetings in which it identifies issues with the quality of its services. NPRC should formally document the information discussed and conclusions reached during the meetings to increase the effectiveness of its monitoring process.

*NIST SP 800-53, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, control PM-4 PLAN OF ACTION AND MILESTONES PROCESS, Supplemental Guidance states: “...With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization.”*

Office of Human Capital

Adopting a competency-based hiring model requires an investment of time and effort up front, but that investment is generally well worth the effort when making hiring decisions. After the hire is made, core competencies continue to be useful in setting goals and positioning new hires for success, identifying areas for professional development, and making appropriate decisions about future promotions and raises. While NARA has used a competency model in its hiring practice, we noted the Office of Human Capital’s (H) Competency model is currently out of date and has not been updated in more than

five years. While NARA's mission has not changed, the skills and competencies required to carry out that mission are continually evolving as NARA increases its focus on digitization and the collection and preservation of electronic records. Without clearly defined competencies, NARA may not be identifying and hiring the most appropriate individuals to fill key positions within the agency.

In addition, we noted management does not have an effective process in place to ensure that personnel provide detailed position descriptions, including the required skill set, to H in a timely manner to assist in the hiring process. H has not prioritized the updating of its existing competency models and has not taken steps to identify an effective solution to ensure that managers communicate the required skills for open positions.

Without an effective process in place to ensure that managers identify and communicate the required skills to the Office of Human Capital before it posts ads for open positions, NARA may not attract or hire the right talent for the positions and may ultimately use its limited resources in an inefficient manner.

#### NARA Project Management

While NARA does offer project management assistance and training, we noted that it only provides these resources upon formal request, and they are not required for certain projects that may present greater risks or challenges for the agency. NARA's current project management policies and procedures which are included in NARA's Capital Planning and Investment Control (CPIC) process are primarily focused on projects that require funding for information technology or for which there is a federally mandated requirement to have project management controls in place. While this process does appear to cover the majority of projects within NARA, there is a risk that critical projects are not captured under this process.

NARA does not have an overarching policy that defines what constitutes high-risk or highly critical projects and includes specific requirements for the administration, tracking, and monitoring of those projects. According to the Project Management Institute (PMI), to improve enterprise performance in implementing strategic projects, organizations are adopting project management best practices.

Without developing, documenting, and implementing formal agency-wide project management requirements, NARA increases its risk that it may not identify, prioritize, or track to completion highly complex, risky, or critical projects. In addition, the lack of minimum project requirements for all NARA projects increases the risk that projects not subject to federal project management requirements will be managed informally, without clear goals or metrics to ensure that the project is efficiently and effectively carried out.

***Suggestions:***

We suggest that the Chief Operating Officer \ Chief Risk Officer ensure NARA Management and Program Offices:

1. Develop, document, and implement requirements to formally identify and document issues relating to NPRC service performance, and to track these issues through resolution.
2. Require NPRC to formally document the results of its weekly meetings to identify key management decisions and to facilitate the identification and tracking of issues.
3. Develop, document, and implement a process to update NARA's competency model on a periodic basis.
4. Develop, document, and implement procedures to ensure that managers clearly communicate the required skill set for open positions before posting the positions.
5. Develop, document, and implement agency-wide project management requirements that:
  - a. Clearly define the criteria for projects to be considered key (e.g., high-risk, highly critical, highly complex, or large-dollar projects).
  - b. Identify and document minimum requirements or best practices that all NARA projects should follow.
  - c. Identify and document minimum requirements for key projects. Requirements could include formal review, approval, and monitoring of projects by NARA senior management; identification of key personnel; training and certification for project managers; and formal status reporting, including key metrics to measure performance of project milestones and deliverables.



## Appendix A – Acronyms and Abbreviations

---

CA	Office of Accountability
COO	Chief Operating Officer
CPIC	Capital Planning and Investment Control
CRO	Chief Risk Officer
EGRC	Enterprise Governance, Risk, and Compliance Program
ERA	Electronic Records Archives
ERM	Enterprise Risk Management
FFMIA	Federal Financial Management Improvement Act
FMFIA	Federal Managers' Financial Integrity Act
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
ICP	Internal Controls Program
IT	Information Technology
MCOO	Management Controls Oversight Council
NARA	National Archives and Records Administration
NGC	NARA General Counsel
NHPRC	National Historical Publications and Records Commission
NIST	National Institute of Standards and Technology
NPRC	National Personnel Records Center
OFR	Office of the Federal Register
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PMI	Project Management Institute
RMF	Risk Management Framework
SP	Special Publication

## Appendix B – Management’s Response to the Report

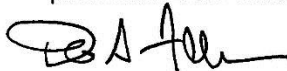
---



Date: OCT 26 2016  
To: James Springs, Inspector General  
From: David S. Ferriero, Archivist of the United States  
Subject: *OIG Draft Report 17-AUD-02, Cotton & Company’s Enterprise-Wide Risk Assessment  
Audit of NARA’s Internal Controls*

Thank you for the opportunity to review and comment on the above referenced draft report. As you know, the field work for this audit was conducted before publication of the revised OMB Circular A-123 (July 2016), which established requirements for Enterprise Risk Management (ERM) in Executive agencies. We believe that most of the findings and recommendations of this audit will assist us in developing a new ERM program at NARA. However, we have left flexibility in our planned actions and target completion dates so that we can address the underlying findings and conclusions supporting your recommendations in a manner that is consistent with OMB’s new standard.

As each recommendation is satisfied, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at [kimm.richards@nara.gov](mailto:kimm.richards@nara.gov) or by phone at 301-837-1668.



DAVID S. FERRIERO  
Archivist of the United States

Attachment

NATIONAL ARCHIVES *and*  
RECORDS ADMINISTRATION  
8601 ADELPHI ROAD  
COLLEGE PARK, MD 20740-6001  
[www.archives.gov](http://www.archives.gov)

**Action Plan Response to OIG Report:**  
**17-AUD-02, Cotton & Company's Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls**

**Recommendation 1a:** The Chief Operating Officer/Chief Risk Officer fully implement all components of NARA 160, including: (a) developing, documenting, and fully implementing NARA 162, *NARA's Enterprise Risk Management Program*. Within NARA 162, roles and responsibilities for ERM activities should be clearly identified.

**Planned Actions:** NARA will issue NARA 162, *NARA's Enterprise Risk Management Program*.

**Target Completion Date:** September 29, 2017

**Recommendation 1b:** The Chief Operating Officer/Chief Risk Officer fully implement all components of NARA 160, including: (b) developing, documenting, and fully implementing NARA 163, *NARA's Issues Management*.

**Planned Actions:** NARA 163, *NARA's Issues Management*, will not be implemented. NARA 160 will be revised to remove any reference to NARA 163.

**Target Completion Date:** September 29, 2017

**Recommendation 2:** The Chief Operating Officer/Chief Risk Officer develop, document, and implement a formal process to: (a) identify and prioritize risks within the organization. Risks should be tied directly to NARA's strategic plan and mission and prioritized based on their overall importance to the agency; and (b) prioritize risk management activities including the use of limited resources based on key risks within the organization. Management's prioritization should be clearly documented and include formal steps to ensure risks are maintained at an appropriate level.

**Planned Actions:** NARA will develop a documented Enterprise Risk Management framework that includes formal processes to ensure that senior leadership identifies and prioritizes appropriate risks, consistent with OMB Circular A-123, and prioritize risk management activities.

**Target Completion Date:** September 29, 2017

**Recommendation 3:** The Chief Operating Officer/Chief Risk Officer provide additional resources to the Office of Accountability to ensure ICP activities are effectively carried out.

**Planned Actions:** NARA will evaluate resource needs to conduct these programs consistent with OMB models for internal controls and risk management.

**Target Completion Date:** September 29, 2017

**Recommendation 4:** The Chief Operating Officer/Chief Risk Officer develop and implement a formal process to review and evaluate the completeness and accuracy of ICP documentation submitted. Validation procedures should include a formal review: (a) to ensure all required documentation has been submitted by the due date. Where documentation has not been provided, NARA should have a formal process in place to follow up and obtain the required documentation; (b) of ICP documentation submitted to ensure it is both complete and accurate. Where discrepancies are identified, NARA should have a formal process in place to follow up with management so corrections can be made; (c) of each office's submission to determine whether risks identified and conclusions made are appropriately supported; (d) of test plans and test results for all high-risk or highly critical functions to ensure they clearly demonstrate the office's methodology for performing testing and reaching conclusions; and (e) of monitoring plans and

monitoring results for all functions that clearly show the extent of monitoring performed the office's methodology for performing the monitoring, and the rationale for its conclusions.

**Planned Actions:** NARA will develop an Enterprise Risk Management framework, to include internal controls, that includes processes to ensure that a formal review process addressing items a through e is in place.

**Target Completion Date:** September 29, 2017

**Recommendation 5:** The Chief Operating Officer/Chief Risk Officer develop and fully implement a formal ICP training program. NARA's ICP training program should identify and require individuals who are involved with NARA's ICP to complete initial training and refresher training periodically thereafter. Further, management should track completion of ICP training to ensure all individuals involved in the ICP process have received adequate training.

**Planned Actions:** NARA will develop Enterprise Risk Management training for pertinent staff in FY 2017. This training may include materials specific to internal controls.

**Target Completion Date:** September 29, 2017

**Recommendation 6:** NARA General Counsel develop, document, and fully implement policies and procedures to ensure NARA personnel (i.e., employees, contractors, and others with access to NARA systems or information) review and formally acknowledge their responsibilities to comply with NARA's privacy rules of behavior annually.

**Planned Actions:** NARA will update IT Security and PII training for FY 2017 to include an acknowledgment of rules of behavior.

**Target Completion Date:** September 29, 2017

**Recommendation 7:** NARA General Counsel implement a process for following up on outstanding system change inquiries and obtaining the requested information.

**Planned Actions:** NGC will develop a process and institute controls to reasonably ensure that responses are received to outstanding system change inquiries. Results will be incorporated into NARA's internal control program reporting.

**Target Completion Date:** September 29, 2017

**Recommendation 8:** NARA General Counsel Develop, document, and implement policies and procedures to periodically test the effectiveness of privacy policies, procedures, and controls

**Planned Actions:** NARA will develop, document and implement monitoring and testing plans to reasonably ensure the effectiveness of privacy policies, procedures and controls; consistent with applicable NIST 800-53A guidance. Monitoring and testing plans and results will be incorporated into NARA's internal control program reporting.

**Target Completion Date:** September 29, 2017

## **Appendix C – Report Distribution List**

---

Archivist of the United States  
Deputy Archivist of the United States  
Chief Operating Officer