



May 4, 2010

ROSS PHILO
EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER

JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY SOLUTIONS

DEBORAH J. JUDY
DIRECTOR, INFORMATION TECHNOLOGY OPERATIONS

CHARLES L. MCGANN
MANAGER, CORPORATE INFORMATION SECURITY

SUBJECT: Audit Report – Certification and Accreditation Process
(Report Number IS-AR-10-008)

This report presents the results of our self-initiated audit of the U.S. Postal Service's Certification and Accreditation (C&A) process (Project Number 09RG032IS000). The objective was to determine whether the C&A process for critical applications is effective in identifying and mitigating risks in a timely manner. This audit addresses operational risk. See [Appendix A](#) for additional information about this audit.

Postal Service policy requires management to complete the C&A process for all sensitive-enhanced,¹ sensitive,² and critical information resources to include certification, accreditation, and approval before deployment into the production environment. This formalized process ensures an application has adequate security controls to manage risk throughout the application's life cycle. Key objectives of the C&A process are to assess threats, define security requirements and controls, test security solutions, and evaluate the security controls and processes for the application.

Conclusion

The Postal Service's implementation of the C&A process for critical applications is not effective in identifying and mitigating risks in a timely manner. Management can strengthen the C&A process by providing Corporate Information Security (CIS) the authority necessary to ensure the process is completed for critical applications before

¹ Handbook AS-805, Section 3-2.3.2, Sensitive-Enhanced Information – includes hardcopy or electronic information or material that is not designated as classified but warrants or requires enhanced protection.

² Handbook AS-805, Section 3-2.3.3, Sensitive Information – includes hardcopy or electronic information or material that is not designated as classified or sensitive-enhanced but warrants or requires protection.

deployment, applications are recertified when required, and high residual risks³ are mitigated.⁴ Further, management should ensure C&A documentation is maintained in a central location and the C&A information is updated in the [REDACTED]

We consider two findings identified in this audit report – C&A Process and C&A Documentation and Maintenance – as repeat findings of similar issues identified in prior U.S. Postal Service Office of Inspector General (OIG) reports.⁵ Management agreed with the prior findings and, subsequently, closed the related recommendations in their formal tracking system. See [Prior Audit Coverage](#) for additional information related to these reports.

C&A Process

Management deployed at least 22⁶ applications, classified as critical to Postal Service operations, into production before completing the required C&A process. In addition, management did not recertify applications within required timeframes. Policy⁷ requires recertification for critical applications every 3 years, unless the application must comply with Payment Card Industry (PCI) Data Security Standard (DSS)⁸ requirements, when annual recertification is required.

Management classified 77 production applications as critical to Postal Service operations.⁹ The following table displays the C&A process status for the 77 critical production applications.

³ Residual risk is the risk that remains after management has taken action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk. If the risks are categorized as high, the risk must be mitigated by using a continuous process that reduces risk by implementing cost-effective security measures.

⁴ We calculated a non-monetary impact of approximately \$360 million for data at risk of loss [REDACTED] application. See [Appendix C](#) for the non-monetary impact calculation.

⁵ OIG report *Information Security Assurance Process* (Report Number IS-AR-06-009, dated May 4, 2006) and report *Information Systems Disaster Recovery Process* (Report Number IS-AR-04-004, dated March 10, 2004).

⁶ We identified 22 applications that were placed in production without completed C&As – the eight In Progress, nine Not Started (see [Table 1](#)), and five of the sample applications we reviewed (see [Table 3](#)). However, this list may not be all inclusive as we did not perform a comprehensive review of all 77 critical applications.

⁷ Handbook AS-805, Section 8-4.1, What the C&A Process Covers, and Section 8-5.7.9, Re-Initiate C&A.

⁸ The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. As of September 5, 2006, the Postal Service was required to comply with these standards.

⁹ A classification of critical is given to applications classified as critical to Postal Service operations. If the application supports one of six functions – for example, protecting customer or employee life, safety, or health – the application will receive a critical classification.

Table 1: C&A Process Status

C&A Process Status	Applications
Completed	60
In Progress	8
Not Started	9
Total	77

In addition, 23 of the 60 applications with completed C&As were overdue for recertification. Seven of the 23 must comply with PCI annual recertification requirements. See [Appendix D](#) for a complete list of applications in each category.

We judgmentally selected eight applications, from the 60 with completed C&As, for further detailed review. Five of the eight applications were deployed into production before completing the C&A process.

The CIS is responsible for managing the C&A process;¹⁰ however, CIS does not have the authority necessary to enforce and execute the responsibilities when dealing with individuals outside the CIS reporting structure or whose positions are more senior within the organization. Further, policy does not require C&A training for the vice presidents, executive sponsors, or portfolio managers who are involved in the C&A process. As a result, these individuals may not be aware of their role and responsibility when conducting the C&A or understand the magnitude of the risks they are willing to accept on behalf of the Postal Service. In addition, portfolio managers and executive sponsors are not held accountable for incorporating the C&A process and the required documentation into the application's Technology Solutions Life Cycle (TSLC) process.

In response to a similar finding in a prior audit report,¹¹ management agreed to complete the Information Security Assurance (ISA)¹² process for applications already placed in production. On May 4, 2006, management closed the related recommendation in their formal tracking system; however, because this issue continues to exist, we consider this a repeat finding. When the C&A process is incomplete, management increases the potential for disclosure of sensitive data that may negatively impact the Postal Service brand. See [Appendix B](#) for our detailed analysis of this topic.

¹⁰ Handbook AS-805, Section 2-2.4 (e.), Manager, Corporate Information Security Office.

¹¹ U.S. Postal Service Office of Inspector General (OIG) report, *Information Security Assurance Process* (Report Number IS-AR-06-009, dated May 4, 2006).

¹² In 2008, CIS changed the ISA process to the C&A process to align it with terminology other federal agencies use. The C&A process and required documentation is incorporated into the TSLC process and should be conducted concurrently with the development and deployment of new information resources.

We recommend the executive vice president and chief information officer:

1. Provide Corporate Information Security the authority necessary to enforce and execute the responsibilities for managing the Certification and Accreditation process.

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

2. Update Handbook AS-805, *Information Security*, to require mandatory annual training on the Certification and Accreditation process for all portfolio managers.
3. Ensure all portfolio managers receive mandatory training regarding their role, responsibility, and accountability for implementing and reinitiating the Certification and Accreditation process. This training should also be made available to all executive sponsors.
4. Hold portfolio managers accountable to complete the Certification and Accreditation process within the Technology Solutions Life Cycle prior to implementing critical applications into the production environment.
5. Complete the Certification and Accreditation process for all critical applications currently in production, as required by Handbook AS-805, *Information Security*.
6. Ensure the portfolio managers work with the executive sponsors to initiate the recertification process for critical applications assigned to their functional areas as required by Handbook AS-805, *Information Security*.

Unmitigated Residual Risks

Management could not provide evidence that all high residual risks were mitigated for critical applications in production as agreed to during the C&A process. Specifically, management could not provide documentation to indicate risks were mitigated for seven of the eight production applications reviewed. For example, the risk mitigation plan (RMP) for the [REDACTED] listed multiple high-risk vulnerabilities that were scheduled to be mitigated by October 31, 2007. However, management could not provide documentation to show they mitigated these risks.

Policy¹³ allows the portfolio managers and executive sponsors to review the RMP, accept the residual risks, and approve the application for deployment. However, there is no formal, centralized mechanism to track the status of residual risks identified in the RMP. Further, no single entity is held accountable for tracking these risks and ensuring they are resolved as stated in the RMP and recertification letter. As a result,

¹³ Handbook AS-805, Section 8-5.7.1, Executive Sponsor and Portfolio Manager Make Decision to Deploy.

management cannot ensure critical production applications are adequately protected to prevent security threats and vulnerabilities. Unauthorized disclosure or misuse of information could result in significant financial loss that may have a negative impact on the Postal Service brand. We quantified the risks associated with the [REDACTED] at approximately \$360 million in non-monetary [REDACTED]

[REDACTED] See [Appendix B](#) for our detailed analysis of this topic and [Appendix C](#) for our non-monetary impact calculation.

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

7. Develop a formal, centralized mechanism to track the status of all unmitigated residual risks identified in the applications' risk mitigation plan.
8. Input unmitigated residual risks identified in the applications' risk mitigation plan into the formal, centralized tracking mechanism and track the risks through resolution.

We recommend the manager, Corporate Information Security, coordinate with the vice president, Information Technology Solutions, and the director, Information Technology Operations, to:

9. Work with executive sponsors to resolve unmitigated residual risks identified in the risk mitigation plans and recertification letters associated with the critical applications.

C&A Documentation and Maintenance

Management is not consistently maintaining C&A documentation in the TSLC Artifacts and CIS Team Documents libraries or updating the status of key C&A documentation in the EIR.

- The TSLC Artifacts and CIS Team Documents libraries are repositories that contain finalized project deliverables for all technology solutions. At present, management maintains C&A documentation in both locations. However, we were unable to locate a completed C&A documentation package in either location for the 60 applications listed in the EIR as having completed the C&A process. Policy does not designate either library as the official repository for storing the

[REDACTED]

C&A documentation. Policy also does not assign a single entity responsible for maintaining the C&A documentation.

- The EIR is a repository that provides centralized access to the application's information to include designated fields for entering key information instrumental to the C&A process. However, information entered in the fields was inconsistent, inaccurate, or missing. Although management attempted to assign responsibility for maintaining application information in the EIR in policy;¹⁵ no single entity is held accountable for updating and validating information related to the C&A process.

Management agreed to add the C&A documentation to an online repository in a previous OIG report.¹⁶ In addition, management agreed to resolve inconsistencies in the EIR data in two previous reports.¹⁷ Although management has closed each of the applicable recommendations from the prior reports, these issues continue to exist. Therefore, we consider these issues repeat findings. By resolving these issues, management could simplify the C&A process – making the process more effective and efficient – and ensure gaps in the C&A process are identified to make timely and credible decisions for securing and managing these applications. See [Appendix B](#) for our detailed analysis of this topic.

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

10. Establish policy to designate a central repository for storing the Certification and Accreditation documentation.
11. Update Handbook AS-805, *Information Security*, to designate a single entity responsible for uploading the Certification and Accreditation information in the central repository for all critical applications.
12. Input the Certification and Accreditation documentation for all critical applications into the central repository.
13. Update Handbook AS-805, *Information Security*, to designate a single entity for updating and validating the Certification and Accreditation information in the Enterprise Information Repository for all critical applications.

Management's Comments

¹⁵ Handbook AS-805, Section 2-2.11, Portfolio Managers, Section 2-2.29, Information Systems Security Officers, Section 3-3.3, Recording Information Resource Classification and Categories of Information Processed, Section 9-9.3, Relationship of Criticality, Recovery Time Objective, and Recovery Point Objective, and Section 9-9.5, Information Resource Recovery and Reconstitution.

¹⁶ OIG report *Information Security Assurance Process* (Report Number IS-AR-06-009, dated May 4, 2006).

¹⁷ OIG report *Information Security Assurance Process* (Report Number IS-AR-06-009, dated May 4, 2006) and report *Information Systems Disaster Recovery Process* (Report Number IS-AR-04-004, dated March 10, 2004).

Management agreed with the 13 recommendations. In response to recommendation 1, management stated that the CIS manager has the responsibility to manage and administer the C&A process. In addition, it is the manager, Corporate Information Technology (IT) Portfolios, and the director, IT Operations', responsibility to perform the task assignments. Management believes this line of authority is in place and, therefore, requested closure of this recommendation.

To address recommendations 2 and 3, management will update Handbook AS-805, *Information Security*, to reflect the requirement for the manager, Corporate IT Portfolios, and the director, IT Operations, to require mandatory training on the C&A process for all portfolio managers and staff. Management will provide this training annually. The targeted completion dates are December 31, 2010, for recommendation 2 and September 30, 2010, for recommendation 3.

In response to recommendation 4, management stated that proper completion of the C&A requirements are already part of the TSLC; however, management will add additional compliance monitoring to ensure the TSLC process is followed. Targeted completion date is immediately for new critical application production implementations.

To address recommendations 5 and 6, management will complete the C&A process, including the recertification process, for all critical applications. The exceptions will be the various Enterprise Data Warehouse (EDW) Datamarts that are covered by the EDW Infrastructure Impact Assessment. The targeted completion date for both recommendations is March 31, 2011.

To address recommendations 7 through 9, CIS will research and implement an automatic tracking system to enter all unmitigated risks cited in the application's risk mitigation plan. Once successfully implemented, CIS will use the automatic tracking system functionality to notify the manager, Corporate IT Portfolios, and the director, IT Operations, of their responsibilities to perform the task assignments and work with the executive sponsor to resolve unmitigated risks associated with the application identified in the risk mitigation plan. The targeted completion date for these recommendations is December 31, 2010.

In response to recommendations 10 through 12, CIS will update Handbook AS-805-A, *Information Resource Certification & Accreditation Process*, to reflect the requirement for the manager, Corporate IT Portfolio, and the director, IT Operations, to designate and utilize the TSLC Artifacts library as the central repository for storing C&A documentation. Portfolio program managers will also be responsible for, and will input, C&A information to the TSLC Artifacts Library. The targeted completion date for recommendations 10 and 11 is December 31, 2010. The targeted completion date for recommendation 12 is immediately per existing TSLC responsibilities.

In their original response to recommendation 13, management stated Handbook AS-805-A, *Information Resource Certification & Accreditation Process*, Section 2-6 (g)

currently outlines this requirement. Specifically, policy states executive sponsors are responsible for ensuring the C&A documentation package is securely stored and kept current for the information resource life cycle. Management stated this process is currently in place and, therefore, requested closure of this recommendation.

See [Appendix E](#) for management's comments in their entirety.


In a subsequent discussion with the OIG, management amended their comments to recommendation 13 to state that they will update the handbook to indicate the portfolio program manager is responsible for updating the EIR with status of the C&A for all critical applications. The targeted completion date is December 30, 2010.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and their corrective actions should resolve the issues identified in the report. However, we do not agree that recommendation 1 should be closed at this time. We support management's decision to designate the manager, CIS, be responsible for executing the C&A process. However, it is imperative that the manager also be given the authority to enforce the requirements with individuals outside his work group. We believe a reliable gauge to measure the success of this effort will be the CIS manager's ability to successfully complete the C&A process for all critical applications by the March 31, 2011, targeted completion date specified in management's response to recommendation 5. This recommendation will remain open until management can provide evidence that the intent of the recommendation has been met.

The OIG considers recommendations 1 through 13 significant and, therefore, requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Frances E. Cain, director, Information Technology, or me at 703-248-2100.

E-Signed by Darrell E. Benjamin, Jr. 
VERIFY authenticity with ApproveIt

Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Sally K. Haring

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

Postal Service policy requires management to complete the C&A process for all sensitive-enhanced, sensitive, and critical information resources to include certification, accreditation, and approval before deployment into the production environment. This formalized process ensures an application has adequate security controls to manage risk throughout the application's life cycle. Key objectives of the C&A process are to assess threats, define security requirements and controls, test security solutions, and evaluate the security controls and processes for the application.

A C&A documentation package is required for the information resource, which includes a consolidation of the business impact assessment (BIA), vulnerability and risk assessment, security plan, contingency plan, and the security test and evaluation (ST&E) plan. To determine the criticality of the application, a BIA is prepared to ensure compliance with privacy requirements, sensitivity and criticality, and appropriate security requirements.

CIS is responsible for managing the C&A process and providing guidance on application security. The Corporate Information Technology and Field Applications Portfolios are responsible for supporting executive sponsors in developing the application and completion of the C&A process. After completing the certification process, the executive sponsor and the portfolio manager may decide to deploy the application even though high and/or moderate unmitigated residual risks remain. However, the executive sponsor and portfolio manager should jointly determine whether the residual risks are acceptable, and, if so, prepare and sign a conditional acceptance letter and approve the application for deployment.

OBJECTIVE, SCOPE, AND METHODOLOGY

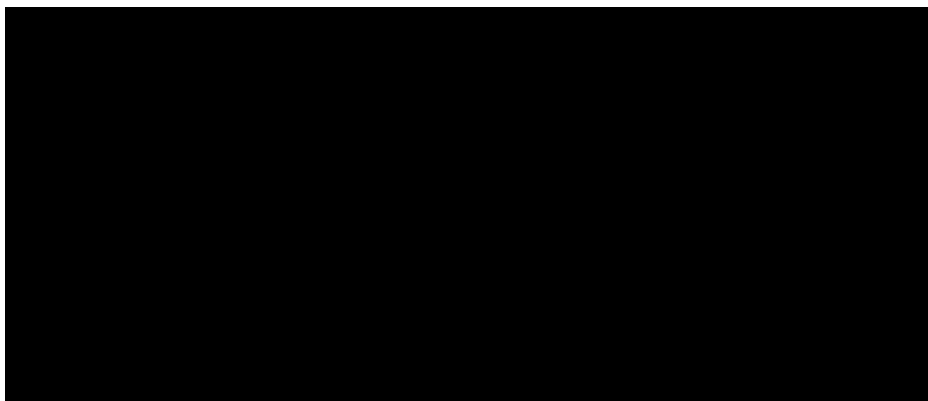
Our objective was to determine whether the C&A process for critical applications is effective in identifying and mitigating risks in a timely manner. To accomplish this objective, we reviewed the status of the C&A process for critical applications assigned a risk criticality of "high" and deployed into production. Specifically, we reviewed critical applications in the following C&A categories:

- Completed.
- In progress.
- Not started.
- Recertification in process.

To further review the status of the C&A process, we judgmental selected a sample of eight applications from the 60 critical applications identified as having completed C&As.

The table below lists the eight applications in our sample and identifies the applications that are in-scope for PCI and Sarbanes Oxley (SOX) compliance.

Table 2: Sampled Applications



We reviewed C&A documentation included in the TSLC Artifacts and CIS team documents libraries for all critical production applications. The documentation reviewed included the BIA, security plan, ST&E plan, contingency plan, RMP, risk assessment and vulnerability scans, certification letter, accreditation letter, acceptance letter, conditional C&A letter, and recertification letter, if applicable. We also reviewed the residual risks identified for the eight applications selected to determine whether management mitigated risks according to the RMP and recertification letter. In addition, we reviewed management's process for tracking the residual risks identified for applications deployed into production.

Finally, we reviewed applicable C&A policies, procedures, roles and responsibilities, and interviewed key officials representing CIS, Corporate IT Portfolios, the Field Applications Portfolio, Business Continuity Management, and business owners from multiple functional areas.

We conducted this performance audit from September 2009 through May 2010 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We reviewed computer generated data from the EIR and determined the data was unreliable for the purpose of conducting this audit. We discussed our observations and conclusions with management on March 26, 2010, and included their comments where appropriate.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date Report	Results
<i>Information Security Assurance Process</i>	IS-AR-06-009	May 4, 2006	Although the Postal Service has made progress in clearing the backlog of ISA projects and implemented a comprehensive vulnerability testing program, further effort is needed to ensure the ISA processes are completed timely. Management should address issues related to EIR data accuracy, consistency, reliability, availability, and the need for a central location for storage. The report also noted managers had the ability to deploy systems before completing the ISA process. We made three recommendations to the Postal Service to complete the required deliverables for the applications identified as having missing documentation, to expedite the population of the online repository, and validate the reliability of the EIR data. Management agreed with and closed the recommendations in their formal tracking system on May 4, 2006; September 27, 2007; and December 8, 2006, respectively.
<i>Information Systems Disaster Recovery Process</i>	IS-AR-04-004	March 10, 2004	Managers do not always update EIR data elements for disaster recovery. Data elements such as the BIA, application disaster recovery plan status, and testing information were missing or inaccurate. We recommended the Postal Service develop a process to enforce current policy to update the EIR data and improve the quality of data currently maintained in the EIR. Management agreed and closed the recommendation in their tracking system on November 5, 2004.

APPENDIX B: DETAILED ANALYSIS

C&A Process

Management deployed at least 22 critical applications into production before completing the C&A process. In addition, management did not recertify applications as required. Management identified 77 production applications with a critical classification of “high.” See [Appendix D](#) for details on the 77 critical applications.

Policy¹⁸ requires management to complete the full C&A process for all critical resources, culminating with the certification, accreditation, and approval documents for deploying the information resource. All three documents are required before placing the application into production. Policy¹⁹ also requires recertification for critical applications every 3 years and every year for applications that must comply with the PCI DSS requirements.

We judgmentally sampled eight applications for further review from the 60 critical applications with a completed C&A. As table 3 illustrates, management deployed five applications into production – [REDACTED] before completing the C&A process. In addition, the recertification is past due for five applications – [REDACTED]

Table 3: Sampled Applications C&A Status

Application	Deployment Date	C&A Process Completion Date ²⁰	Recertification Due Date*	Deployed Prior to C&A Completion
[REDACTED] 05-27-1995		07-09-2009 07-09-2012		
[REDACTED] 10-01-1987	1-2005	03-19-2008	03-19-2009 X	
[REDACTED] 07-30-2007	01-15-2008	06-17-2009 06-17-2014	01-15-2009 X	
[REDACTED] 10-01-1985		06-17-2009 06-17-2014		
[REDACTED] 05-12-1999		03-19-2003 ²¹	07-25-2007 X	
[REDACTED] 04-26-2001	11-18-2008		11-18-2009 X	
[REDACTED] 02-29-2000		None	02-24-2008 X	

*Shading has been added to identify those applications whose recertification dates are past due.

Although responsible for managing the C&A process, CIS does not have the authority necessary to enforce and execute the responsibilities when dealing with individuals outside the CIS reporting structure or whose positions are more senior within the

¹⁸ Handbook AS-805, Section 8-4.1, What the C&A Process Covers.

¹⁹ Handbook AS-805, Section 8-5.7.9, Re-Initiate C&A.

²⁰ The EIR lists [REDACTED] as legacy applications. The Postal Service placed these applications into production before the current C&A process. As a result, the original certification documentation was unavailable for these applications.

²¹ The EIR did not list a C&A Process Completion Date for [REDACTED]; however, the acceptance of accreditation letter for [REDACTED] was dated March 19, 2003.

organization. Further, policy does not require C&A training for the vice presidents, executive sponsors, or portfolio managers who are involved in the C&A process. As a result, these individuals may not be aware of their role and responsibility when conducting the C&A process or understand the magnitude of the risks they are willing to accept on behalf of the Postal Service. Over a 5-month period in 2009, CIS offered C&A training to managers involved in developing applications in an effort to educate them on their roles and responsibilities in the C&A process. However, manager attendance was optional and, as a result, only few attended.

In addition, portfolio managers and executive sponsors are not held accountable for incorporating the C&A process and required documentation into the TSLC process. Each of the seven phases of the TSLC has corresponding security activities that management must perform to maintain a secure environment. The C&A process and required documentation is incorporated into the TSLC process and conducted concurrently with the development and deployment of new information resources.

Table 4: TSLC Phases and Required C&A Documentation

TSLC Phases	C&A Required Documents
Initiate and Plan	EIR
Requirements BIA	Questionnaire
Analysis and Design	C&A Recertification Letter, Risk Assessment, and Security Plan
Build Not	Applicable
System Integration Test	ST&E Plan and conduct security test
Customer Acceptance Test	Accreditation Letter, Risk Acceptance Letter, Certification Letter, RMP, C&A Acceptance Letter
Release Not	Applicable

Because these issues continue to exist, we consider them repeat findings. As a result, management increases the risk for potential disclosure of sensitive data such as credit card data or personal identifiable information that may negatively impact the Postal Service brand. See [Appendix A](#), Prior Audit Coverage, for details on the prior OIG reports.

Unmitigated Residual Risks

Management could not provide evidence that high residual risks were mitigated for critical applications in production as agreed to during the C&A process. Once the C&A process is complete, the portfolio manager reviews the certification letter and the supporting C&A documentation and escalates security concerns or prepares a RMP for any residual risks rated “medium” or “high”, recommending whether the risks should be accepted, transferred or further mitigated. If a documented vulnerability will not be mitigated, the portfolio manager and executive sponsor should prepare and sign an

acceptance of responsibility letter. In addition, the portfolio managers should work jointly with the executive sponsor to review the C&A documentation package, accept the residual risk, and approve the application for production or return the application to the applicable life cycle phase for rework.

Management could not provide documentation indicating they mitigated risks for seven of the eight production applications in our sample. For example:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

■ Management can perform vulnerability scans to identify risks and to determine whether the residual risks associated with the application are mitigated. Vulnerability scans evaluate applications for vulnerabilities and compliance with Postal Service information security policies and standards. Scans are recommended for all applications and required for applications that require PCI compliance.

In January 2009, CIS began tracking the RMP for critical applications by using a spreadsheet maintained on a desktop computer. The spreadsheet is an informal, decentralized mechanism that does not afford portfolio managers and executive sponsors access to the RMP information. For example, six of the eight applications in our sample are not currently included on the RMP tracking spreadsheet. The CIS manager receives the spreadsheet monthly and, in turn, provides a copy to the vice president, IT Business Solutions. While we commend management's initiative, no single entity is held accountable for tracking these risks and ensuring they are resolved as stated in the RMP and recertification letter. As a result, management cannot ensure critical production applications are adequately protected to prevent security threats and vulnerabilities.

C&A Documentation and Maintenance

Management is not consistently maintaining C&A documentation in the TSLC Artifacts, and CIS Team Documents libraries or updating the status of key C&A documentation in the EIR. Currently, management maintains C&A documentation in two locations – the TSLC Artifacts and CIS Team Documents libraries. Although, we found C&A documents in these libraries, we were unable to locate a complete C&A documentation package for any of the 60 applications identified as having completed the C&A process. Specifically, of the 60 applications, we could not locate the following documents in either of the two libraries:

Table 5: Missing C&A Documentation

C&A Documents	Number of Applications with Missing Documents	Percentage
Approved BIA	21	35
Security Plan	50	83
Risk Assessment	53	88
ST&E Plan	50	83
Vulnerability Scan	58	97
Contingency Plan	35	58
Certification Letter	52	87
RMP 51		85
Acceptance Letter/Risk Acknowledgment Letter	49	82
Accreditation Letter	53	88
Recertification Letter	51	85

Further, the following documents were missing for the eight applications in our sample:

Table 6: Missing C&A Documents – Sampled Applications

C&A Documents*	Application Name							
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Approved BIA								
Security Plan	X		X X					
Risk Assessment			X X X					
ST&E Plan			X X			X		
Vulnerability Scan	X X				X	X		
Contingency Plan					X			X
Certification Letter	X		X X					X
RMP	X		X					
Accreditation Letter	X		X X				X	X
Acceptance Letter/Risk Acknowledgment Letter/Conditional	X		X X					X
Recertification Letter		X	X			X		X

*An 'X' indicates the document was missing for that application.

Policy²³ does not designate either the TSLC Artifacts or CIS Team Documents library as the official repository for storing the C&A documentation or assign a single entity responsible for maintaining the C&A documentation. By maintaining the documentation in a central location, management can simplify the C&A process, making it more efficient and effective, and ensure gaps are identified, which will help protect critical applications from security threats and vulnerabilities.

The EIR is a repository that provides centralized access to the application's information to include designated fields for entering key information instrumental to the C&A process. However, information entered in the fields was inconsistent, inaccurate, or missing. For example,

- [REDACTED]
- [REDACTED]

²³ OIG report *Information Security Assurance Process* (Report Number IS-AR-06-009, dated May 4, 2006).

- [REDACTED]

Policy²⁴ states portfolio managers should ensure applications are entered in the EIR and updated as required. The ISSOs should ensure the responsible project manager records the sensitivity and criticality designation in the EIR. The initial determination of criticality for an information resource is determined during the BIA process. Management should update the EIR when the BIA is completed. While management attempted to assign responsibility for maintaining accurate application information in the EIR in policy, no single entity is held accountable for updating and validating information related to the C&A process. Therefore, management cannot rely on the EIR information to make timely and credible decisions for securing and managing these applications.

Because these issues continue to exist, we consider these repeat findings. See [Appendix A](#), Prior Audit Coverage, for details on the prior OIG reports.

²⁴ Handbook AS-805, Section 2-2.11, Portfolio Managers, Section 2-2.29, Information Systems Security Officers, Section 3-3.3, Recording Information Resource Classification and Categories of Information Processed, Section 9-9.3, Relationship of Criticality, and Recovery Time Objective, and Recovery Point Objective.

APPENDIX C: NON-MONETARY IMPACT

The following presents an estimate of the potential costs the Postal Service could incur due to [REDACTED]

[REDACTED] We based the total non-monetary impact of \$359,984,152 on a 1 day average of [REDACTED] multiplied by a cost of \$62 per transaction. The calculation assumes each transaction may contain at least one element of sensitive and critical information when, in fact, each transaction could contain more than one piece of sensitive and critical information.

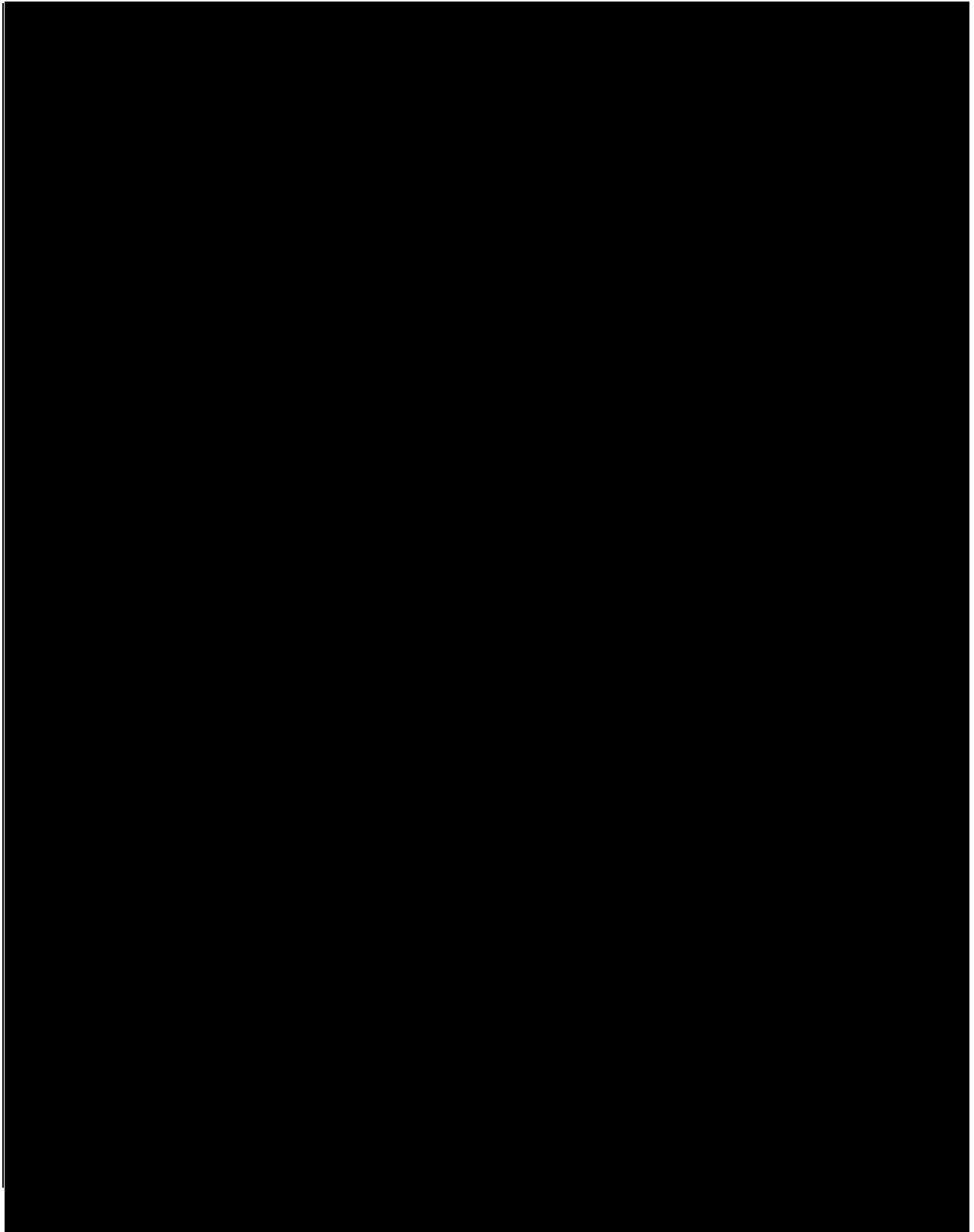
Cost Category	Costs per Record Affected as Reported by Ponemon Institute²⁶
Detection and Escalation	
Internal Investigation, Legal, Audit, and Consulting	\$ 8
Notification	
Letters, Email, Telephone, Published Media, and Website	\$ 15
Ex-Post Response	
Mail, Email, Telephone (to Internal Call Center), Telephone (to Outsourced Call Center), Legal Defense, Criminal Investigations (forensics), Public or Investor Relations, Free or Discounted Services	\$ 39
Total	\$ 62²⁷

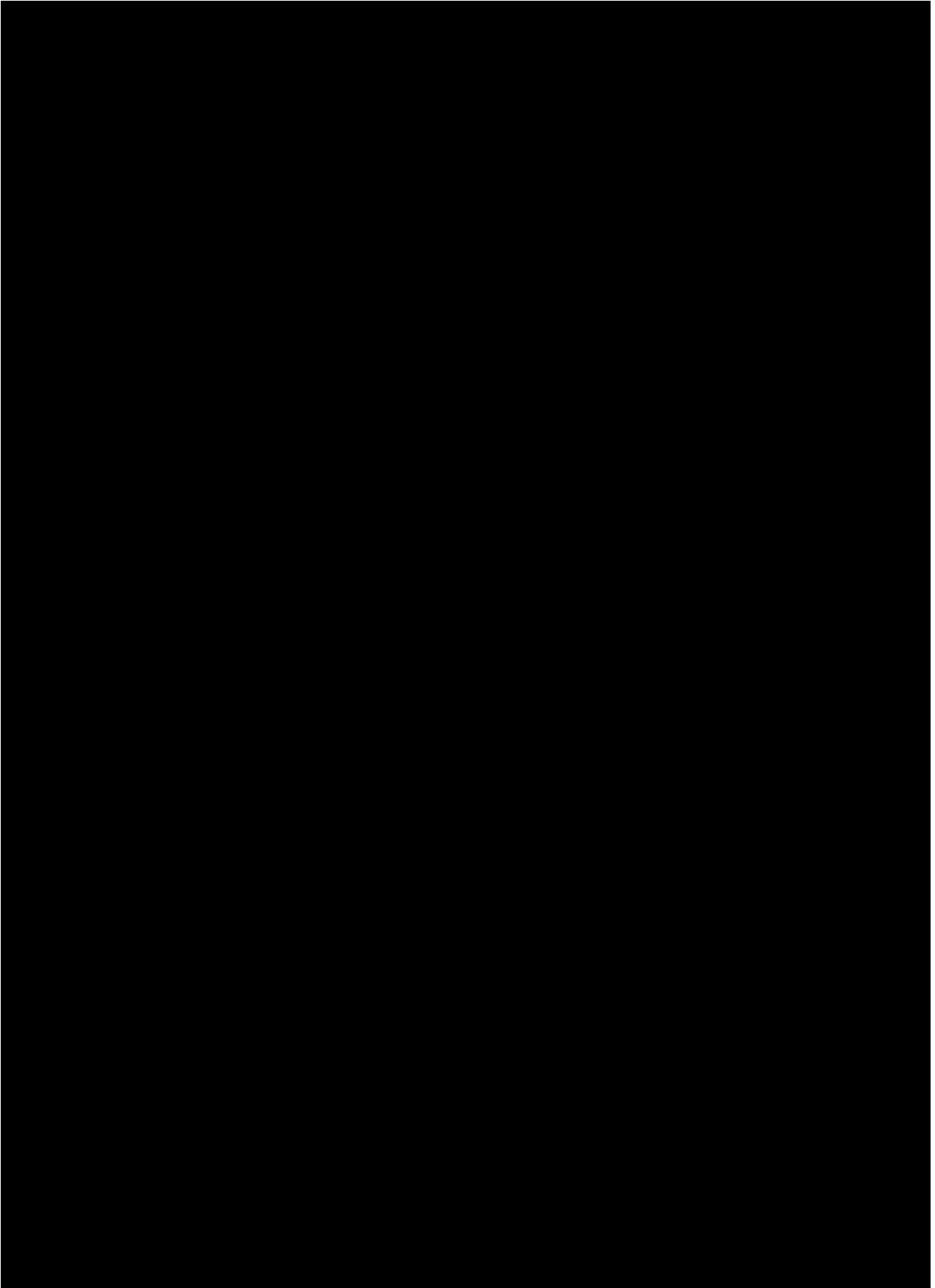
²⁵ [REDACTED]

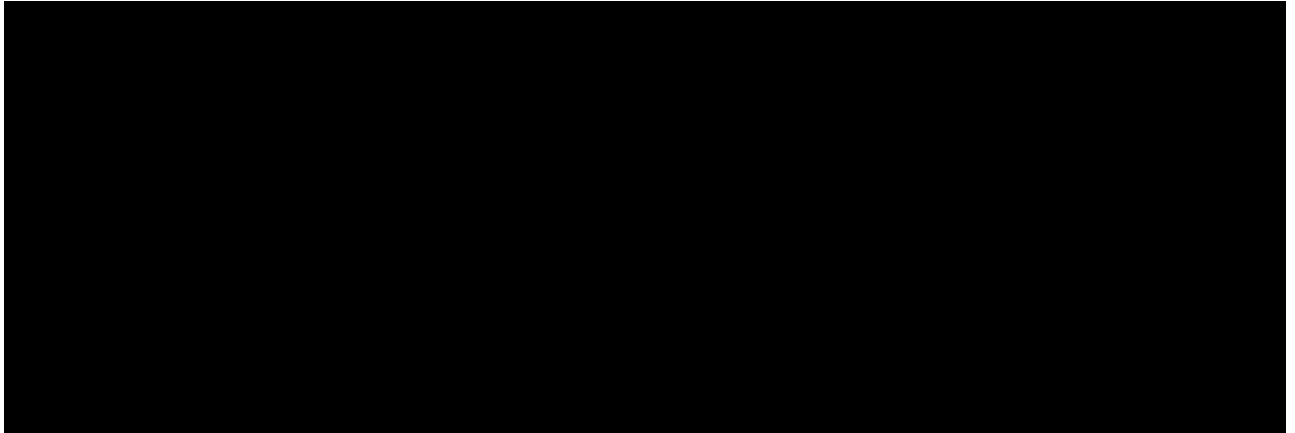
[REDACTED]
Ponemon Institute, LLC, *Fourth Annual US Cost of Data Breach Study*, dated January 2009. Ponemon Institute conducts independent research on privacy, data protection, and information security policy.

²⁷ The Ponemon Institute study reports the total cost per breach as \$202; however, \$139 of the costs contributed to lost business, which we determined is not applicable. These figures are exactly as those the Ponemon Institute reported. We attribute the \$1 difference (\$63 versus \$62) to rounding the figures within each category.

APPENDIX D: C&A STATUS FOR 77 CRITICAL PRODUCTION APPLICATIONS







APPENDIX E: MANAGEMENT'S COMMENTS

ROSS PHILO
Executive Vice President
Chief Information Officer



April 27, 2010

Lucine M. Willis
Director, Audit Operations
Office of Inspector General
1735 N. Lynn Street, Room 11044
Arlington, VA 22209-2020

SUBJECT: Transmittal of Draft Audit Report – Certification and Accreditation Process
(Report Number IS-AR-10-DRAFT), Project Number 09RG032IS000

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 1 through 13 of the report; the response is attached.

The subject report and this response contain information related to potential security vulnerabilities that, if released, could possibly be exploited and cause substantial harm to the U.S. Postal Service. The Manager, Corporate Information Security will work with you to determine what portions of this report should be considered as classified and restricted and exempt from disclosure under the Freedom of Information Act.

If you have any questions or comments regarding this response please contact Gerri Wallace, Corporate Information Security at (202) 268-6821.

Ross Philo

Attachment

cc: John T. Edgar
Deborah H. Judy
Charles L. McGann
Sally K. Haring

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1500
202-268-6900
FAX: 202-268-4492
ROSS.PHILO@USPS.GOV
WWW.USPS.COM

Certification and Accreditation Process
(Report Number IS-AR-10-FRAFT) Project Number 09RG032IS000
Page #2

We recommend the executive vice president and chief information officer:

1. Provide Corporate Information Security the authority necessary to enforce and execute the responsibilities for managing the Certification and Accreditation process.

Management agrees with the recommendation. The manager, Corporate Information Security, currently has the responsibility to manage the Certification and Accreditation (C&A) process. It is with the intent of this finding to designate a group or manager that is 100% responsible for the entire process. Vice President, Information Technology Solutions, agreed that it is the manager, Corporate Information Security's responsibility to administer the C&A process, and it is the manager, Corporate Information Technology Portfolios, and the director, Information Technology Operations', responsibility to perform the task assignments.

Anticipated completion date: Currently in place, requesting closure upon receipt of this report.

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

2. Update Handbook AS-805, *Information Security*, to require mandatory annual training on the Certification and Accreditation process for all portfolio managers.

Management agrees with the recommendation. CISO will update Handbook AS-805, *Information Security*, to reflect the requirement for the manager, Corporate IT Portfolios' team, and the director, Information Technology Operations, to require mandatory annual training on the Certification and Accreditation process for all portfolio managers and staff.

Anticipated completion date: December 31, 2010

3. Ensure all portfolio managers receive mandatory training regarding their role, responsibility, and accountability for implementing and reinitiating the Certification and Accreditation process. This training should also be made available to all executive sponsors.

Management agrees with the recommendation. Training will be provided annually based on the response provided for recommendation #2.

Anticipated completion date: September 30, 2010 -annually

4. Hold portfolio managers accountable to complete the Certification and Accreditation process within the Technology Solutions Life Cycle prior to implementing critical applications into the production environment.

Management agrees with the recommendation. Proper completion of Certification and Accreditation requirements are part of the TSLC today. Additional compliance monitoring will be added to ensure it is followed.

Anticipated completion date: Immediately for new critical application production implementations.

5. Complete the Certification and Accreditation process for all critical applications currently in production, as required by Handbook AS-805, *Information Security*.

Certification and Accreditation Process
(Report Number IS-AR-10-FRAFT) Project Number 09RG032IS000
Page #3

Management agrees with the recommendation. Certification and Accreditations will be completed for all critical applications for which one has not been done. The exceptions will be the various EDW Datamarts that are covered by the EDW Infrastructure Impact Assessment (IIA).

Anticipated completion date: March 31, 2011

6. Ensure the portfolio managers work with the executive sponsors to initiate the recertification process for critical applications assigned to their functional areas as required by Handbook AS-805, *Information Security*.

Management agrees with the recommendation. Recertification will be completed for all critical applications, as required.

Anticipated completion date: March 31, 2011

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

7. Develop a formal, centralized mechanism to track the status of all unmitigated residual risks identified in the applications' risk mitigation plan.

Management agrees with the recommendation. CISO will research and implement an automatic tracking system to enter all unmitigated risk cited in the application's risk mitigation plan.

Anticipated completion date: December 31, 2010

8. Input unmitigated residual risks identified in the applications' risk mitigation plan into the formal, centralized tracking mechanism and track the risks through resolution.

Management agrees with the recommendation. CISO will research and implement an automatic tracking system to enter all unmitigated risk cited in the application's risk mitigation plan.

Anticipated completion date: December 31, 2010

We recommend the manager, Corporate Information Security; coordinate with the vice president, Information Technology Solutions, and the director, Information Technology Operations, to:

9. Work with executive sponsors to resolve unmitigated residual risks identified in the risk mitigation plans and recertification letters associated with the critical applications.

Management agrees with the recommendation. Once successfully implemented, CISO will use the automatic tracking system functionality as the mechanism to notify the manager, Corporate IT Portfolios' team and the director, Information Technology. It will be the responsibility of the manager, Corporate IT Portfolios' team and the director, Information Technology Operations, to perform the task assignment and work with the executive sponsor to resolve unmitigated risk associated with the application identified in the risk mitigation plan.

Anticipated completion date: December 31, 2010

Certification and Accreditation Process
(Report Number IS-AR-10-FRAFT) Project Number 09RG032IS000
Page #4

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

10. Establish policy to designate a central repository for storing the Certification and Accreditation documentation.

Management agrees with the recommendation. CISO will update Handbook AS-805-A, *Information Resource Certification & Accreditation Process*, to reflect the requirement for Corporate IT Portfolios' team, and the director, Information Technology Operations to designate and utilize the central repository for storing Certification and Accreditation documentation on the Corporate Technology, TSLC Artifacts Library.

Anticipated completion date: December 31, 2010

11. Update Handbook AS-805, *Information Security*, to designate a single entity responsible for uploading the Certification and Accreditation information in the central repository for all critical applications.

Management agrees with the recommendation. Portfolio Program managers are responsible for uploading Certification & Accreditation information to the TSLC Artifact Library.

Anticipated completion date: December 31, 2010

12. Input the Certification and Accreditation documentation for all critical applications into the central repository.

Management agrees with the recommendation. Portfolio Program managers will input Certification and Accreditation information into the TSLC Artifact Library.

Anticipated completion date: Immediately, per existing TSLC responsibilities.

13. Update Handbook AS-805, *Information Security*, to designate a single entity for updating and validating the Certification and Accreditation information in the Enterprise Information Repository for all critical applications.

Management agrees with the recommendation. Handbook AS-805-A, *Information Resource Certification & Accreditation Process*, Section 2-6.G currently outlines this requirement, please reference insert below:

2-6 Executive Sponsors

The executive sponsors, as representatives of the VPs of the functional Business areas, are responsible for ensuring the completion of all security related tasks throughout the life cycle of an information resource. Some information resources are developed under the direction of one executive sponsor in one organization and transferred to an executive sponsor in another organization for production. Executive sponsors are responsible for the following:

(g) *Ensuring that the C&A documentation package is securely stored and kept current for the information resource life cycle.*

Anticipated completion date: Currently in place, requesting closure upon receipt of this report.