EC-Council Licensed Penetration Tester

Methodology: Vulnerability Analysis

Penetration Tester:			
Organization:			
Date:		**Location:**	

PENETRATION

LICENSED

TESTER

[Insert System Name/Acronym]

Vulnerability Categorization: [Insert Vulnerability Categorization]

Vulnerability Assessment Summary Report

Version [Insert #]

[Insert Date]

Prepared by

[Insert Group/Organization/Company Name]
[Insert Street Address]
[Insert City, State, and Zip Code]

DOCUMENT CHANGE CONTROL

Version	Release Date	Summary of Changes	Addendum Number	Name
[Version 0.1]	[Insert Date]	[First Draft]	[Insert Addendum #]	[Insert Name]
[Version 0.9]	[Insert Date]	[Final Draft]	[Insert Addendum #]	[Insert Name]
[Version 1.0]	[Insert Date]	[Final]	[Insert Addendum #]	[Insert Name]

TABLE OF CONTENTS

[This sample format provides a template for preparing a Vulnerability Assessment Summary Report for systems. The template is intended to be used as a guide, and the preparer should modify the format as necessary to comply with internal policies. Where practical, the guide provides instructions [in blue, bolded text] for completing specific sections.

1. EXECUTIVE SUMMARY

The **[Insert System Name/Acronym]** system has been determined to be a **[Insert Major or Minor]** System and has been determined to have a vulnerability categorization of **[Insert High, Moderate, or Low]**.

The periodic assessment of risk to agency operations or assets resulting from the operation of an information system is an important activity required by FISMA. The **[Insert Group/Organization/Company Name]** team prepared this Vulnerability Assessment Summary Report in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems. The results captured within this Report are intended to be an addition to any existing Risk Assessments performed outside of the Certification and Accreditation (C&A) process. It summarizes the risks associated with the vulnerabilities identified during the system's Security Test & Evaluation (ST&E), Privacy Impact Assessment (PIA), e-Authentication Risk Assessment, audits, and any other risk assessment activities. This VAR also serves as the ST&E Report referenced in NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. All results were analyzed to provide the Certifier with an assessment of the management, operational, and technical controls implemented to protect the confidentiality, integrity, and availability of the system, as documented in the System Security Plan (SSP). Table 1 below provides the total number of system-specific security risks, by risk level and control category.

Table 1: Summary of System Security Risks

[Populate this table using the data in Table 12. Insert the number of risks for each control category and risk level. Also, include total numbers for each column and row.]

	Control Category			
Risk Level	**Management**	**Operational**	**Technical**	**Total**
High				
Medium				
Low				
Total				

In certain instances, the system may not have the technical capability to implement a security control or the system owner may make a risk-based decision not to implement a control based on the cost or feasibility of implementing the control relative to risk. Status of such controls is documented as risk-based in the SSP. A summary of these controls and justification for each are provided in Table 2.

Table 2: Summary of Risk Based Decisions

[Populate this table using controls in the SSP that have been designated as Risk Based Decisions. DO NOT USE TBD or N/A. None is an appropriate answer if there are no Risk Based Decisions for the system.]

Management, Operational, or Technical	Control Identifier	Description	Justification

All **[Insert Group/Organization/Company Name]** systems rely on certain organizational controls that are implemented at the Enterprise Level (e.g. Security Policies). Risks relating to these organizational controls should be considered assessing the system's security posture. Table 3 provides the total number of **[Insert Group/Organization/Company Name]** organizational security risks, by impact level and control category. Please refer to Appendix G for more details regarding the organizational level risks.

Table 3: Summary of Organizational Security Risks

	Control Category			
Risk Level	**Management**	**Operational**	**Technical**	**Total**
High				
Medium				
Low				
Total				

Note: The detailed results of the organizational common controls are documented in the accompanying **[Insert Group/Organization/Company Name]** Organizational Common Controls Vulnerability Assessment Report (VAR) dated **[Insert Date]**. These common controls are updated and assessed annually for each FISMA year.

Table 4 provides a summary of the audit findings specific to the system.

Table 4: Summary of System Audit Findings

[Populate this table using applicable audit Reports for the system. DO NOT USE TBD or N/A. None is an appropriate answer.]

Audit Finding	Date of Audit	Reported by	Associated NIST

			Control Family

Table 4a provides a summary of the audit findings related to the Organizational Common Controls.

Table 4a: Summary of Organization Level Audit Findings

[Populate this table using applicable audit Reports for the organization. DO NOT USE TBD or N/A. None is an appropriate answer.]

Audit Finding	Date of Audit	Reported by	Associated NIST Control Family

Table 4b provides a summary of **[Insert Group/Organization/Company Name]** material weaknesses related to computer security.

Table 4b: Summary of Computer Security Material Weaknesses

[Populate this table with any computer security material weaknesses that have been identified for the organization. DO NOT USE TBD or N/A. None is an appropriate answer.]

Material Weakness	Domain(s)	Associated NIST Control Family

Due to the inherent relationship between the system and the underlying General Support System(s) (GSS), GSS risks may impact the overall system security posture. A summary of the GSS risks is provided in Table 5 for the system owner to consider when making the accreditation decision. For more information on the risks that were identified for the GSS(s) and status of the mitigation of these risks, refer to the respective Plan of Action and Milestones (POA&M) for the GSS(s).

Table 5: Summary of GSS Security Risks

[Populate this table using applicable C&A results for each GSS which supports the system. Obtain the list of supporting GSSs from the "Interconnection" table in section 2.15 of the SSP. DO NOT USE TBD or N/A. None is an appropriate answer.]

GSS	GSS Accreditation Status/Date	Date of GSS POA&M	NIST Control Families with Vulnerabilities Identified / Number of POA&M Items (per NIST Control Family)

In order to provide a more holistic view of the risks to the system, [Insert Group/Organization/Company Name] included the GSS components directly supporting the system within the scope of the ST&E. The purpose of including these GSS components as part of the system ST&E is to specifically identify GSS-level risks that may impact the security posture of the system, providing the Designated Approving Authority (DAA) with a higher level of assurance in making an accreditation decision for the system. The scope of the system ST&E included the following GSS components: [include a listing of system-specific GSS components that were tested]. For more information on the risks identified for the GSS components, refer to Table 12a and the ST&E matrix listed in Appendix C of the report. Table 5a provides a summary of the risks identified for the GSS components directly supporting the system.

Table 5a: Summary of Risks Identified for GSS Components Directly Supporting [Insert System Acronym]

[Populate this table using applicable C&A results for system-specific GSS components which were tested as part of the system C&A effort. DO NOT USE TBD or N/A. None is an appropriate answer if no GSS risks were identified.]

GSS	GSS Component	NIST Control Families with Vulnerabilities Identified / Number of POA&M Items (per NIST Control Family)

Refer to the [Insert System Acronym] Certification Memorandum for the accreditation recommendation.

2. INTRODUCTION

The **[Insert System Name/Acronym]** system has been determined to be a **[Insert Major or Minor]** System and has been determined to have a vulnerability categorization of **[Insert High, Moderate, or Low]**.

The periodic assessment of risk to agency operations or assets resulting from the operation of an information system is an important activity required by FISMA. **[Insert Group/Organization/Company Name]** prepared this Vulnerability Assessment Summary Report in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems. It summarizes the risks associated with the findings identified during the system's Security Test & Evaluation (ST&E), Privacy Impact Assessment (PIA), e-Authentication Risk Assessment, audits, and any other risk assessment activities. This report also serves as the ST&E Report referenced in NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

2.1 System Description

[Insert description of the business purpose of the system and system environment, as described in the system's System Security Plan. In addition, include a reference to the SSP for more information about the system. Ensure this section is continuously updated with the latest description from the System Security Plan.]

2.2 Purpose

The purpose of this Vulnerability Assessment Summary Report is to provide the Certifier and the Designated Approving Authority with a more holistic view of risk regarding the system. It documents the Vulnerability assessment activities that were performed on the system and the results of those activities including ST&E, PIA, e-Authentication Risk Assessment, audits, and any other risk assessment activities. This report provides the system's stakeholders with an assessment of the adequacy of the management, operational, and technical controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits or processes.

2.3 Scope

The scope of the report includes the assessment of the system level management, operational, and technical controls as documented in the system SSP and the GSS components that directly support the system. The evaluation of the controls provided by the GSS(s) on which the system resides are documented in the individual GSS C&A packages. A summary of the GSS risks are provided in Tables 5 and 5a for the DAA to consider when making the accreditation decision. Additionally, controls considered to be common security controls, as defined in NIST SP 800-53, were assessed. The results of the assessment of these common controls are summarized in Table 3 in the Executive Summary section of this report.

The following system components were assessed in this report: **[Bullet point components of the system that were assessed and listed in the boundary scope memo – see example below.]**

- **App-X Module 1**
- **App-X Module 2**

The following GSS components that directly support the system were also assessed in this report: **[Bullet point GSS components that directly support the system which were assessed and listed in the boundary scope memo – see example below.]**

- **UNIX Server (GSS X)**
- **Oracle Database Server (GSS X)**

2.4 Structure

The remainder of the Report is structured as follows:

- Section 3 – provides an overview of Vulnerability Assessment Methodology
- Section 4 – provides a summary of Risk Assessment Results
- Section 5 – contains the Accreditation Recommendation
- Appendices provide the detailed findings from the ST&E, PIA, e-Authentication Risk Assessment, and Audits

3. METHODOLOGY

This section describes the methodology used to conduct the vulnerability assessment for the system. The methodology consists of the following steps:

- Step 1. Identify Threats
- Step 2. Identify Vulnerabilities
- Step 3. Analyze Risks
- Step 4. Identify Recommended Corrective Actions
- Step 5. Document Results

3.1 Step 1: Identify Threats

This step begins with compiling a threat statement listing potential threat-sources that are applicable to the system.

3.1.1 Threat Statement Listing

Table 6 provides an overview of the threat sources considered for the system risk assessment.

Table 6: Threat Source List

Identifier	Source and Type	Capabilities	Threat Scenarios	Intentions/Motivations	Resources
T-01	Foreign Intelligence Service over the Internet	Outsider • Highest level of sophistication	• Hacking • Impersonation • Social Engineering • System Intrusion, Break-ins • Unauthorized system access	Malicious • Political Gain • Economic Gain • Military Gain	Substantial • (i.e., Government Financed)
T-02	Terrorist over the Internet	Outsider • Highest level of sophistication	• Hacking • Impersonation • Social Engineering • System Intrusion, Break-ins • Unauthorized system access	Malicious • Political Gain • Economic Gain • Military Gain • Denial of Service • Threaten Harm to Individuals • Create Chaos	Substantial • (i.e., Government Financed)
T-03	Organized Crime over the Internet	Outsider • Highest level of sophistication	• Hacking • Impersonation • Social Engineering • System Intrusion, Break-ins • Unauthorized system access	Malicious • Economic Gain • Political Gain	Moderate to Substantial

Table 6: Threat Source List

Identifier	Source and Type	Capabilities	Threat Scenarios	Intentions/Motivations	Resources
T-04	Individual Hacker over the Internet	Outsider • Many levels of sophistication	• Hacking • Social Engineering • System Intrusion, Break-ins • Unauthorized system access	Malicious • Challenge • Ego • Rebellion • Create Chaos	Minimal to Moderate
T-05	Disgruntled Former Employee over the Internet	Outsider • Many levels of sophistication	• Hacking • Social Engineering • System Intrusion, Break-ins • Unauthorized system access	Malicious • Revenge • Curiosity • Ego • Monetary Gain	Minimal to Moderate
T-06	Disgruntled Employee – System administrator, Engineering team • Local (physically on-site) via Intranet (within the firewall)	Insider • High degree of technical sophistication	• Unauthorized Access • Browsing Proprietary Information • Fraud and Theft • Input of Falsified /Corrupt Information • Sabotage	Malicious • Revenge • Curiosity • Ego • Monetary Gain	Moderate
T-07	Disgruntled Employee – Technical support personnel • Local (physically on-site) via Intranet (within the firewall)	Insider • High degree of technical sophistication	• Unauthorized Access • Browsing Proprietary Information • Fraud and Theft • Input of Falsified /Corrupt Information • Sabotage	Malicious • Revenge • Curiosity • Ego • Monetary Gain	Moderate
T-08	Cleaning crew, service repair crew • Local (physically on-site) and via Company Intranet (within the firewall)	Insider • Many levels of technical sophistication	• Social Engineering • System Intrusion, Break-ins • Unauthorized system access	Malicious • Curiosity • Ego • Monetary Gain	Moderate
T-09	Careless clerical employee • Local (physically on-site) and via Company Intranet (within the firewall)	Insider • Rudimentary degree of technical sophistication	• Input of Corrupt Information	Non-Malicious • Unintentional Errors and Omissions	Minimal

3.2 Step 2: Identify Vulnerabilities

The goal of this step is to develop a list of the system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. The identification of vulnerabilities can take many forms based on various types of risk assessments. The following was used to determine the vulnerabilities within the system—

- The ST&E was used to determine the completeness and effectiveness of the system's security controls. Appendix C provides a detailed listing of findings.
- The Privacy Impact Assessment was utilized to determine the system's compliance with federal Privacy requirements. Appendix D provides a detailed listing of findings.
- The e-Authentication Risk Assessment was utilized to determine the system's compliance with federal e-Authentication requirements. Appendix E provides a detailed listing of findings.
- Vulnerability Risk Assessments and Engineering Risk Based Reviews were reviewed, if available, to determine risks identified as part of the System Development Lifecycle or as part of a separate technical evaluation.

Findings identified as part of the above-mentioned risk assessment activities were reviewed and grouped into risks by NIST SP 800-53 control families or by findings that were related to one another. Additionally, during the consolidation process, findings were grouped by NIST SP 800-53 management, operational, and technical control classes in order to facilitate the process of Reporting risks in Table 1 of this document.

3.3 Step 3: Analyze Risk

The risk analysis for each vulnerability consists of assessing the threats and compensating controls to determine the likelihood that vulnerability could be exploited and the potential impact should the vulnerability be exploited. A general depiction of the analysis is shown in Figure 1, where risk is the intersection of a threat and vulnerability, influenced by likelihood and impact:

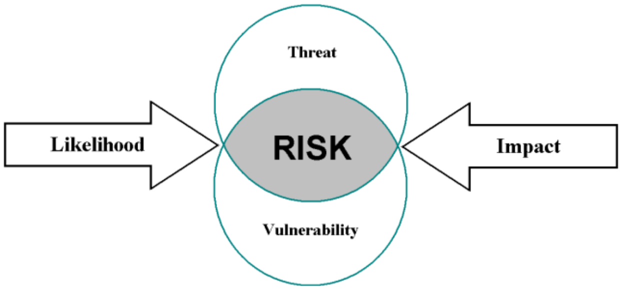

Figure 1. Link Between Likelihood, Impact and Risk

Essentially, risk is proportional to both likelihood of exploitation and possible impact. The following sections provide a brief description of each component used to determine the risk.

3.3.1 Likelihood

The likelihood that a given vulnerability will be exploited by a threat is determined by analyzing the effectiveness of compensating controls against the threat capability. Compensating controls consist of measures in place that assist in mitigating the magnitude of a given vulnerability. Threat capability is defined as the means, opportunity, and motive of a given threat agent. Threat capabilities are defined in Table 7.

Table 7: Threat Capability Components

Component	Description
Means	Means is the mechanism for fulfillment in exploiting the vulnerability. Threat agents are continuously achieving a higher level of means due to the level of sophistication available in easily obtained intrusion tools.
Opportunity	The opportunity for attack is determined by the threat agents' level of access to the system. One of the greatest opportunity differences between threat agents is an insider versus an outsider to the organization, with the insider having far more opportunity to exploit vulnerabilities.
Motive	The motive of a threat agent is his or her desire to exploit vulnerability. Motive can be influenced by the sensitivity of data, desire for monetary gain, or the potential publicity implications of an attack against a highly visible organization.

Once the threat capability and compensating control effectiveness is assessed, for the vulnerability, the overall likelihood of the threat exploiting the vulnerability is determined using the matrix in Table 8.

Table 8: Likelihood Matrix

	Compensating Control Effectiveness		
Threat Capability	Low	Medium	High
High	High	High	Medium
Medium	Medium	Medium	Low
Low	Low	Low	Low

The likelihood of the vulnerability being exploited is the intersection of the threat capability category and the compensating control effectiveness category. For example, if the compensating control effectiveness is "High," the resulting likelihood of exploitation is "Medium" likelihood for a "High" threat capability, "Low" likelihood for a "Medium" threat capability. Table 9 shows the definitions for each likelihood level. Note that a "High" effectiveness for compensating controls cannot completely reduce the likelihood of exploitation of a "High" capability threat.

Table 9: Likelihood Descriptions

Likelihood	Description
High	The capability of the threat is significant, and compensating controls to reduce the probability of vulnerability exploitation are insufficient
Medium	The capability of the threat is medium, and implemented compensating controls lessen the probability of vulnerability exploitation.
Low	The capability of the threat is limited, and compensating controls are in place that effectively reduces the probability of vulnerability exploitation.

3.3.2 Impact

Impact refers to the magnitude of potential harm that may be caused by successful exploitation. It is determined by the value of the resource at risk, both in terms of its inherent (replacement) value, its importance (criticality) to business missions, and the sensitivity of data contained within the system. The results of the system security categorization estimations for each system, discussed in each system's respective SSP, is used as an aid to determining individual impact estimations for each finding. The level of impact is rated as High, Medium, or Low and a description for each level of impact is provided in Table 10.

Table 10: Impact Definitions

Magnitude of Impact	Impact Definitions
High	Exercise of the vulnerability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate	Exercise of the vulnerability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Table 10: Impact Definitions

Magnitude of Impact	Impact Definitions
Low	Exercise of the vulnerability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

3.3.3 Risk Level

The risk level for the finding is the intersection of the likelihood value and impact value as depicted in Table 11.

Table 11: Risk Level Matrix

	Impact		
Likelihood	High	Moderate	Low
High	High	Medium	Low
Medium	Medium	Medium	Low
Low	Low	Low	Low

3.4 Step 4: Identify Recommended Corrective Actions

The finding and associated risk level was used to determine the recommendations that should be applied as a means to mitigate the risk. When identifying recommendations, the following were taken into consideration: level of effort, costs, emerging technologies, time constraints, and feasibility.

3.5 Step 5: Document Results

The results of the risk assessment were documented providing the finding, business impact statement, recommended corrective actions, likelihood, impact, and risk level. Refer to section 4.0 of this report for the risk assessment results.

4. RISK ASSESSMENT RESULTS

This section documents the technical and non-technical security risks to the system. These risks have been determined by applying the methodology outlined in Section 3 of this document to the vulnerabilities identified by the various security reviews that have been performed for the system (as applicable - ST&E, PIA, e-Authentication Risk Assessment, and any other risk assessment activities). The security risks identified in this section largely constitute the basis for the accreditation recommendation provided in Section 5 of this document.

The risk assessment results for the system are documented in Tables 12 and 12a. The following provides a brief description of the information documented in each column:

- **Identifier:** Provides a unique number used for referencing each vulnerability.
- **Source:** Indicates the source where the vulnerability was identified (e.g., ST&E, PIA, e-Authentication Risk Assessment, or any other risk assessment activities.)
- **Risk:** Provides a brief description of the risk.
- **Business Impact Statement:** Indicates the impact to the business of a threat exploiting the vulnerability. The following are examples of potential impacts to business data that could be realized by the exploitation of an system vulnerability:
    - Completeness: All transactions that occurred are entered and accepted for processing by the system.
    - Accuracy: Transactions are properly recorded, and on a timely basis (in the proper period); key data elements input for transactions are accurate and data elements are processed accurately by systems that produce reliable results.
    - Validity: All recorded transactions actually occurred (are real), relate to the organization, and were approved by designated personnel.
    - Confidentiality: System data and Reports are protected against unauthorized access.
- **Recommended Corrective Action:** Provides a brief description of the corrective action(s) recommended for mitigating the risks associated with the finding.
- **Likelihood:** Provides the likelihood of a threat exploiting the vulnerability. This is determined by applying the methodology outlined in Section 3 of this document.
- **Impact:** Provides the impact of a threat exploiting the vulnerability. This is determined by applying the methodology outlined in Section 3 of this document.
- **Risk Level:** Provides the risk level (high, medium, low) for the vulnerability. This is determined by applying the methodology outlined in Section 3 of this document.

The risks identified in the table below are based on security vulnerabilities from various sources including ST&E, PIA, e-Authentication Risk Assessment, and any other risk assessment activities. The security vulnerabilities from the ST&E are listed in the finding matrix in Appendix C of the report. These findings are based on the ST&E results that are documented in the ST&E Plan.

Also, please refer to the source documents (e.g., PIA, e-Authentication Risk Assessment) included in the C&A package for more detailed information on the risks associated with non-ST&E findings.

Table 12: Risk Assessment Results

[Ensure that all risks that were identified as part of risk assessment activities (i.e., ST&E, PIA, e-Authentication Risk Assessment, and any other risk assessment activities) are listed in the table below. Ensure that the "Impact" level for all risks identified in Table 12 is the same as the security categorization level for the system.]

Identifier	Source	Risk	Business Impact Statement	Recommended Corrective Action	Likelihood	Impact	Risk Level
R-01.	**EXAMPLE:** **App-X ST&E Findings Matrix** **AU-2 (App)**						
R-02.							
R-03.							
R-04.							

Identifier	Source	Risk	Business Impact Statement	Recommended Corrective Action	Likelihood	Impact	Risk Level
R-05.							

Supporting GSS Component Risks

Table 12a provides a list of risks that were identified for the GSS components directly supporting the system that may impact the security posture of the system. The GSS components directly supporting the system that were included within the scope of the system ST&E are as follows: **[include a listing of system-specific GSS components that were tested]**. The risks identified in the table below were not included in the total count of risks tallied in Table 1: Summary of System Security Risks. These risks will be incorporated into the respective GSS POA&M(s).

Table 12a: Supporting GSS Component Risk Assessment Results

[Populate this table using applicable C&A results for system-specific GSS components which were tested as part of the system C&A effort. Ensure that the "Impact" level for all risks identified in Table 12a is the same as the security categorization level for the GSS that the risk was identified for. DO NOT USE TBD or N/A. None is an appropriate answer if no GSS risks were identified.]

Identifier	Source	Risk	Business Impact Statement	Recommended Corrective Action	Likelihood	Impact	Risk Level
R-GSS-01.	**EXAMPLE:** **App-X ST&E Findings Matrix** **RA-5 (GSS X Windows 2003 Server)**						
R-GSS-02.							

Mitigated Results

Table 12b provides a list of the risks that were identified in the results of risk assessment activities where actions have been taken to mitigate these risks after risk assessment activities were performed. The **[Insert Group/Organization/Company Name]** Issue Resolution Process was used to confirm that each of the ST&E findings noted below have been mitigated. Therefore, these risks are provided in this report for informational purposes only and do not have an impact on the accreditation recommendation.

Table 12b: Mitigated Results

[Populate the table below with risks that have been mitigated (i.e., ST&E and SRA risks that have been corrected). Any risks that have not been mitigated should be placed in Table 12 above and should not be placed in this table. DO NOT USE TBD or N/A. None is an appropriate answer if a SRA was not performed.]

Identifier	Source	Risk	Business Impact Statement	Recommended Corrective Action	Likelihood	Impact	Risk Level
R-01.	**EXAMPLE:** **App-X SRA, dated 01/02/07** **R-01** **CM-2**						
R-02.	**EXAMPLE:** **App-X ST&E Findings Matrix** **IA-2 (App)**						

5. ACCREDITATION RECOMMENDATION

[Populate this section based on the risks identified in this report and include a reference to the system's Certification Memorandum for the accreditation recommendation. The following is an example:

A total of nine system risks were identified for App-X. Of the nine risks, two were deemed as Medium and seven were deemed as Low. The risks identified in Section 4, Table 12 within this report included weaknesses in the area of Access Controls and Identification and Authentication. Please refer to the App-X Certification Memorandum for the accreditation recommendation.]

The Federal Information Security Management Act (FISMA) requires that a Plan of Action and Milestones (POA&M), using the format guidance prescribed by OMB, be utilized as the primary mechanism for tracking all system security weaknesses and issues. The authorizing official (accreditor), will need to take ownership of these risks and ensure they are included in the weakness repository and that the POA&M for the system is updated, monitored, and progress Reported quarterly through your FISMA coordinator.

5.1 Priority Mitigation Actions

[Complete this section if there are major mitigation actions that must be completed. Otherwise, remove this section in its entirety. This section must be completed for any systems issued an IATO.]

Each item in the POA&M is important for the overall security of the system. Nevertheless, a smaller set of changes is required to merit Authorization to Operate under guidelines documented in NIST Special Publication 800-37. These items are considered so significant that the Certification Agent is unwilling to recommend unrestricted operation of the system until the vulnerabilities have been substantially corrected. Table 13 presented below depicts the priority mitigation actions for the system. These mitigation actions are subset of what is presented in the system POA&M document.

Table 13: Priority Mitigation Actions

Risk Level	Risk Identifier	Vulnerability Description

6. FUTURE ENHANCEMENTS

The following planned changes to the **[Insert System Acronym]** environment are provided here for informational purposes only. At the time of the current system C&A review, these changes were still in development, and therefore not enough information was available to accurately document and test the security controls planned for implementation with these enhancements. These future enhancements will be documented and tested as part of the next update to the system C&A package.

[If section 5.1 was completed above, change the table below to Table 14.]

Table 13: Future Enhancements

Future Enhancement Title	Future Enhancement Description	Implementation Date(s)

APPENDIX A. ACRONYMS

[Update the acronym list based on the acronyms used in this document]

AC	Authentication Category
AP	Assurance Profile
ATO	Authorization to Operate
C&A	Certification & Accreditation
COTS	Commercial Off the Shelf
DAA	Designated Approving Authority
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
GSS	General Support System
IATO	Interim Authorization to Operate
ID	Identification
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
POC	Point of Contact
RA	Risk Assessment
SA	System Administrator
VAR	Vulnerability Assessment Report
SDLC	System Development Life Cycle
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation

APPENDIX B. REFERENCES

Laws and Regulations:

- Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347.
- Consolidated Appropriations Act of 2005, Section 522.
- USA PATRIOT Act (P.L. 107-56), October 2001.

OMB Circulars:

- OMB Circular A-130, Management of Federal Information Resources, November 2000.
- OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June, 2006.

FIPS Publications:

- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS PUB 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST Publications:

- NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
- NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST 800-30, Risk Management Guide for Information Technology Systems
- NIST 800-34, Contingency Planning Guide for Information Technology Systems
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST 800-53, Recommended Security Controls for Federal Information Systems
- NIST 800-53a, Guide for Assessing the Security Controls in Federal Information System
- NIST 800-60, Guide for Mapping Types of Information and Information Systems to Security
- NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
- NIST 800-64, Security Considerations in the Information System Development Life Cycle

[Insert System Acronym] References

- **[Insert any business-related laws/regulations that apply to the system].**

APPENDIX C. SECURITY TEST AND EVALUATION (ST&E)

An ST&E was performed on **[Insert Dates]** at **[Insert Location]** for the system. The results of the ST&E are presented in the completed ST&E plan which is part of the C&A package. The security vulnerabilities identified during the ST&E are provided below. Testing against the system and GSS components that directly support **[Insert System Acronym]** operations was conducted. The ST&E for the system included the following components: **[Bullet point components of the system that were assessed and listed in the boundary scope memo – see example below.]**

- **App-X Module 1**
- **App-X Module 2**

The ST&E for the GSS components that directly support the system included the following: **[Bullet point GSS components that directly support the system which were assessed and listed in the boundary scope memo – see example below.]**

- **UNIX Server (GSS X)**
- **Oracle Database Server (GSS X)**

Vulnerabilities discovered for the system components which were tested are listed under the System Level Findings section in this appendix. Vulnerabilities discovered on the supporting GSS components are listed under the Supporting GSS Component Findings section in this appendix.

Note: Obtain the ST&E Plan and Findings Matrix for the system to complete this appendix. Also, be sure to roll up duplicate findings and place finding statement in a list for that specific control in the appropriate component section of the "System Level Findings" table below. For example, if five test cases failed for IA-2, take the unique language in those test cases and put it into an entry for IA-2 under the appropriate component section in the table below (i.e., If an IA-2 test case fails for "App-X Module 1", place the language under this component section in the table. If an IA-2 test case fails for "App-X Module 1", as well as for the "App-X Module 2", split the findings up accordingly and place entries for IA-2 into each of these sections of the table.)

System Level Findings

Vulnerabilities discovered for the system components which were tested are listed in the table below. The composite risks and risk levels for system vulnerabilities are captured in Table 12 of the report along with the business impact statement and recommended corrective actions.

[Populate the table below using the findings identified for system components that were tested as part of the ST&E – see the example below.]

ST&E Control Number and Name	Applicable NIST SP 800-53 Control(s)	ST&E Finding Statement
[Insert name of system component – i.e., App-X Module 1]		

ST&E Control Number and Name	Applicable NIST SP 800-53 Control(s)	ST&E Finding Statement
SA-5: Information System Documentation	The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.	[Insert finding statement from ST&E Results Matrix and failed test case number(s)] EXAMPLE: Adequate documentation for App-X is not maintained. (APP-SA5-01A, APP-SA5-01B)
[Insert name of system component – i.e., App-X Module 2]		
CM-6: Configuration Settings	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	[Insert finding statement from ST&E Results Matrix and failed test case number(s)]

Supporting GSS Component Findings

In order to provide a more holistic view of the risks to the system, **[Insert Group/Organization/Company Name]** included the GSS components directly supporting system within the scope of the system ST&E. The purpose of including these GSS components as part of the ST&E is to specifically identify GSS-level risks that may impact the security posture of the system, providing the DAA with a higher level of assurance in making an accreditation decision for the system. The composite risks and risk levels for the supporting GSS Component vulnerabilities are captured in Table 12a of the report along with the business impact statement and recommended corrective actions. A summary of the GSS risks are provided in Tables 5 and 5a of the report.

[Populate the table below using the findings identified for GSS components that were tested as part of the ST&E – see the example below. DO NOT USE TBD or N/A. None is an appropriate answer if no GSS findings were identified.]

ST&E Control Number and Name	Applicable NIST SP 800-53 Control(s)	ST&E Finding Statement
[Insert name of GSS component – i.e., UNIX Server (GSS X)]		
CM-6: Configuration Settings	**The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.**	**[Insert finding statement from ST&E Results Matrix and failed test case number(s)]**
SI-11: Error Handling	**The information system identifies and handles error conditions in an expeditious manner.**	**[Insert finding statement from ST&E Results Matrix and failed test case number(s)]**
[Insert name of GSS component – i.e., Oracle Database Server (GSS X)]		

ST&E Control Number and Name	Applicable NIST SP 800-53 Control(s)	ST&E Finding Statement
CM-6: Configuration Settings	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	[Insert finding statement from ST&E Results Matrix and failed test case number(s)]
CM-7: Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].	[Insert finding statement from ST&E Results Matrix and failed test case number(s)]

APPENDIX D. PRIVACY IMPACT ASSESSMENT (PIA)

A PIA was performed or revised for the system as part of the C&A activities. A copy of the PIA Risk Memo is presented in this appendix. The security risks identified based on the PIA are documented in a Table 12 of this report.

[Insert PIA Risk Memo here.]

Or

A PIA was performed or revised for the system as part of the C&A activities. A copy of the PIA Risk Memo is presented in this appendix. There were no security risks identified based on the PIA.

[Insert PIA Risk Memo here.]

Or

A PIA is not required for this system. Therefore, a copy of the PIA Risk Memo is not presented in this appendix.

APPENDIX E. E-AUTHENTICATION RISK ASSESSMENT

[Insert System Acronym] has been determined to be a Federal System that does not require e-Authentication security controls to be implemented due to the nature of the transactions processed on the system.

Or

An e-Authentication Risk Assessment was performed or revised for the system as part of the C&A activities. A copy of the e-Authentication Risk Assessment is presented in this appendix. The security risks identified based on the e-Authentication Risk Assessment are documented in Table 12 of this report.

Introduction

The purpose of this e-Authentication Assurance Level Determination Report is to document the e-Authentication risk assessment activities that were performed according to the OMB Presidential Memorandum M-04-04, e-Authentication Guidance for Federal Agencies, December 2003, and Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, and the results of those activities. This Report provides management with an assessment of the assurance impact profile level of electronic system transactions of remote users to ensure that authentication processes provide the appropriate level of assurance.

Overview

An e-Authentication assurance level determination was conducted in accordance with the OMB Presidential Memorandum M-04-04, e-Authentication Guidance for Federal Agencies, December 2003, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline, June 2004, and Federal Information Processing Standards (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

In order to compile a comprehensive review of the systems and their transactions, an interview transpired between the e-Authentication Assurance Risk Assessment Profile Team (Assessment Team), and the point of contact for **[Insert System Name (Acronym)]**. A risk assessment on new and existing electronic transactions was conducted to ensure that current authentication processes provide the appropriate level of assurance.

Scope

This Report incorporates an analysis of the external and internal facing e-Authentication transactions on the following components: **[Insert System Acronym]**.

Structure

The Report is structured as follows:

- Results of the e-Authentication risk assessment;

- Transaction Report provided by the e-Authentication risk assessment tool.

E-AUTHENTICATION RISK ASSESSMENT RESULTS

Assessment Interview Summary

EXAMPLE:

The assessment team performed a telephone interview with on Wednesday, September 21, 2005 at 9:00 AM. The assessment team used the streamlined set of assurance questionnaire worksheets to guide the interview and used a hardcopy of the worksheet to record responses from the interviewees. No notable departures from the worksheet structure occurred.

System Operations

EXAMPLE:

App-X requires authentication for Government Employees over the Organization X Intranet. All users are considered internal users. The number of user sessions in a year are less than 200. The system URL provides the front door information page for the App-X system. Users access the NT App-X System Server by utilizing the workstation's Netscape browser and Organization X Intranet (inside the Organization X firewalls). When the URL for the App-X system is entered, a Java applet is downloaded into the workstation's memory. The user is then prompted for a login id and password combination for the system. If the login id/password combination matches what is stored in the App-X database (password is encrypted in the database) for that user, the system then checks the list of authorized IP addresses (also stored in the database) to determine if the user's workstation is authorized to access App-X. The user is granted access only if the IP address of his/her workstation matches one of the IP addresses allocated to that user. From this point on, the system server passes requests from the client workstation to the App-X database server using Oracle, a commercial off-the-shelf (COTS) software. Users do not have direct access to the App-X database server or to the App-X database at any time.

Transactions

Table 1 provides a summary of the e-Authentication Transaction Worksheet results for **[Insert System Name]**. The Table uses the following six elements to delineate each transaction:

- **ID** – A unique "association" identifier used to link a transaction with all other qualitative elements of the e-Authentication assurance profiling process: security categories (SC), threat statements, vulnerabilities, authentication category impacts, vulnerability likelihood ratings, assurance levels, risk levels, mitigations, and assurance level impact profiles (e.g., A, B, C);
- **Action** – Transaction type: a "verb" (e.g., inquire, create, modify, delete);
- **Asset** – Data object: the object being acted upon by the Actor (e.g., personal profile, tax record, tax credit, employee record);
- **Attributes** – Set, in writing, the apparent authentication characteristics (e.g., sensitivity, privacy, availability, user/group restrictions, non-repudiation needs);
- **Actor** – User type: a "subject" [e.g., citizen, federal agency (FA), business, external filing partner, employee, administrator]; and

- **Avenue** – Entry point: the instrumental vehicle for the transaction (e.g., Internet, registered user portal, employee user portal, intranet, extranet).
- **Authentication Category (AC)** – OMB Authentication Potential Impact Category, or "Authentication Category" (AC) for each transaction. According to OMB M-04-04, categories of harm and impact include:
  AC1 – Inconvenience, distress, or damage to standing or reputation;
  AC2 – Financial loss or agency liability;
  AC3 – Harm to agency programs or public interests;
  AC4 – Unauthorized release of sensitive information;
  AC5 – Personal safety; and
  AC6 – Civil or criminal violations.
- **Assurance Profile (AP) --** The four assurance profile levels for each security category are:
  Level 1: Little or no confidence in the asserted identity's validity.
  Level 2: Some confidence in the asserted identity's validity.
  Level 3: High confidence in the asserted identity's validity.
  Level 4: Very high confidence in the asserted identity's validity.

Table 1. System Transaction Summary

EXAMPLE

							AC						
ID	**Name**	**Action**	**Asset**	**Attributes**	**Actor**	**Avenue**	**1**	**2**	**3**	**4**	**5**	**6**	**AP**
App-X-001	User-Manage Account	Modify	Employee Record	C, I, P, N	Government Employees	Intranet	L	L	L	L	L	M	**3**
App-X-002	User-View Report	Inquire	Employee Record	C, I, P, N	Government Employees	Intranet	L	L	L	L	L	M	**3**
App-X-003	Admin-View Reports	Inquire	Employee Record	C, I, P, N	Government Employees	Intranet	L	L	L	L	L	M	**3**
App-X-004	Admin-Create User Account	Create	Employee Record	C, I, P, N	Government Employees	Intranet	L	L	L	L	L	M	**3**
App-X-005	Admin-Modify User Account	Modify	Employee Record	C, I, P, N	Government Employees	Intranet	L	L	L	L	L	M	**3**

Conclusion

EXAMPLE:

As indicated in Table 1 in the right-most column, labeled "AP," the assurance profile level for this system is a Level 3.

The system has mission-specific transactions which need to be carried out by Organization X users. In addition there is a moderate level of impact resulting from an authentication failure which can lead to civil or criminal violations. This impact is primarily due to the consequences of unauthorized access to the system which can result in unauthorized access to sensitive information. Although only those users who have admin privileges may modify or update this information, there must be a high level of confidence that the individual logging in is indeed the authorized individual.

However, technically at a level 3 assurance level two factor authentication is required such as a one-time password through a cryptographic protocol. The use of an the IP checker which only allows users with authorized IP addresses (stored in the database) to access App-X only if their IP address of their workstation matches one of the IP addresses allocated to that user, provides a mitigation control.

APPENDIX F. AUDIT REPORTS

Audit findings have been identified for the system. Results from the relevant audit Reports are presented in this appendix. The security vulnerabilities identified based on these Reports are documented in a table in section 4 of the report.

[Provide relevant audit Reports here.]

Or

Audit findings have not been identified for the system. As such, no audit Reports are presented in this appendix.

APPENDIX G. ORGANIZATIONAL COMMON CONTROLS VAR

Please refer to the organizational common controls VAR dated **[Insert Date]** for more information.