|  |  |
| --- | --- |
|  | HHS Logo |



|  |
| --- |
|  |

Facility:

External Risk Analysis

|  |
| --- |
|  |

Month/Year Initiated:

**Controlled Unclassified Information**

This information is intended for <INSERT COMPANY’S NAME HERE> internal use only. Once information is added to this template, disclosure outside of <INSERT COMPANY’S NAME HERE> is prohibited without prior authorization and consent of the <INSERT COMPANY’S NAME HERE> Chief Information Security Officer.

**Template Date: July 2013, Revision 5**

**Record of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Change No.** | **Date** | **Name** | **Subject** | **Page No.** |
| 1 | 02/24/2011 | TRD | Added Section 16 | 33 |
| 2 | 02/24/2011 | NMS | Revised Appendix Headings | 24, 25, 27 |
| 3 | 02/24/2011 | TRD | Revised Section 5.2 | 16 |
| 4 | 02/24/2011 | TRD | Revised Template Title | i |
| 5 | 03/04/2011 | TRD | Revised Security Review | 33 |
| 6 | 08/24/2011 | LMB | Revised Section 5.4 | 17 |
| 7 | 10/25/2011 | TD | Revised Section 5.1 and Appendix B | 14, 23 |
| 8 | 12/19/2012 | LB | Removed all references to specific IHS tools |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Contents**

[1.0 Executive Summary 1](#_Toc350424777)

[2.0 Risk Analysis Methodology 2](#_Toc350424778)

[3.0 Introduction 4](#_Toc350424779)

[3.1 Purpose 4](#_Toc350424780)

[3.2 Scope 5](#_Toc350424781)

[3.3 System Characterization 5](#_Toc350424782)

[3.4 Network Architecture Diagram 7](#_Toc350424783)

[4.0 Threat Identification 8](#_Toc350424784)

[5.0 Vulnerability Identification 12](#_Toc350424785)

[5.1 Network Scans <list the tool(s) used> – (Continuous monitoring/monthly reports) 12](#_Toc350424786)

[5.2 Penetration Testing – (Performed Annually) 13](#_Toc350424787)

[5.3 Intrusion Prevention System – <list tools used> (Continuous Monitoring) 14](#_Toc350424788)

[5.4 Wireless Site Survey Tools – (Performed annually) 14](#_Toc350424789)

[5.5 Malware Detection – <list tools used> (Continuous monitoring) 14](#_Toc350424790)

[5.6 Log Management – <list tools used> Periodic review of logs) 15](#_Toc350424791)

[5.7 Other Tools 15](#_Toc350424792)

[6.0 Control Analysis 15](#_Toc350424793)

[7.0 Risk Mitigation Strategies 19](#_Toc350424794)

[8.0 Appendix A: Network Diagram(s) 20](#_Toc350424795)

[9.0 Appendix B: Monthly Network Scan Reports 21](#_Toc350424796)

[10.0 Appendix C: Annual Penetration Test 22](#_Toc350424797)

[11.0 Appendix D: Key Roles in a Risk Assessment 23](#_Toc350424798)

[12.0 Appendix E: Risk Mitigation Worksheet 25](#_Toc350424799)

[13.0 Security Review and Attestation 26](#_Toc350424800)

# Executive Summary

This risk analysis (RA) is designed to assess the security posture of a system or application from the company manager’s viewpoint with the purpose of raising the manager’s awareness of the major security risks in their infrastructure, to propose recommendations for mitigation of these risks, and to ensure <INSERT COMPANY’S NAME HERE> meets the federal requirements for Meaningful Use (MU).

Further, an RA is used to estimate potential losses that could result from system and environmental vulnerabilities and to quantify the damage that may result if certain threats occur. The ultimate goal of the RA is to help select cost-effective safeguards that will reduce the risks to an acceptable level. After the damage from threats is quantified, the manager can determine if

* The cost for a proposed safeguard is reasonable and does not exceed the financial and administrative cost of recovering the information or replacing the system
* The proposed safeguard complies with federal mandates
* The proposed safeguard does not endanger the life of a patient or the interests of the <INSERT COMPANY’S NAME HERE>. Risk management is a management responsibility.

Securing IT systems, data, and physical assets is a never-ending cycle as new technologies and threats emerge. Because threats are constantly changing, conducting an RA continuously helps to ensure that adequate security controls are up-to-date and operating as designed in order to minimize the risk to <INSERT COMPANY’S NAME HERE> and other interconnected government systems.

The MU RA enables the facility to accomplish its mission by ensuring increased security of the Resource and Patient Management System (RPMS), Electronic Health Record (EHR) and other interconnected IT systems that store, process, or transmit patient health information. This document can also help management make well-informed risk management decisions to justify the expenditures that are part of the overall IT systems budget. Finally, this process will help meet the MU requirement for <INSERT COMPANY’S NAME HERE> as described below:

* Conduct or review a security risk analysis as specified in 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

Note that although the completion of this document helps facilities meet the MU measure for conducting a Risk Analysis, facilities must continually strive to “. . . implement security updates as necessary and correct identified security deficiencies as part of its risk management process.” Facilities must work to minimize risk AND mitigate vulnerabilities on a continuous and ongoing basis.

**Note**: This risk analysis is based on the guidelines provided in the Federal Information Processing Standards (FIPS) Publication FIPS-199 [*Standards for Security Categorization of Federal Information and Information Systems*](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf) and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, [*Risk Management Guide for Information Technology Systems*](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf). For a more information about the overall risk management process, see NIST (SP) 800-37, [*Guide for Applying the Risk Management Framework to Federal Information Systems*](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf).

#

# Risk Analysis Methodology

Risk management is the process of identifying, assessing, and taking appropriate steps to reduce threats to an acceptable level. This assessment is the first step in determining potential risks to a facility’s information resources. The overall objective of the RA is to identify IT security weaknesses and to implement adequate cost-effective controls designed to reduce risks to <INSERT COMPANY’S NAME HERE>-owned assets as well as other interconnected systems that may affect the integrity or availability of sensitive patient data.

The RA should consider all physical assets including buildings, workstations, portable media, information systems and their components, along with the information created, transmitted, maintained, or received by the facility. The review should look at the various types of information to determine how important it is, how vulnerable it is, what the cost of losing the information is, and what the cost of protecting it would be. It should be noted, it is difficult to attach a financial cost to the loss of public trust when patient data is lost or compromised but financial cost is a critical factor in the evaluation process. The cost of securing a system should not exceed the total cost of recovering the information or replacing the system unless it is in the interest of patient safety or organizational viability.

There are many methods available to conduct a risk analysis. One method would be to assign a facilitator(s) and staff members representing key aspects of the system or applications being assessed for risk. The makeup of the group will vary depending on the systems and applications involved but may include business and functional program management, system and information owners, senior management, security representatives, privacy officers, general users of the system(s) or application(s), system administrators, and approving officials. This team should work together to identify the assets of the facility, a common set of threats, vulnerabilities and countermeasures for each of the systems, information and applications being evaluated as part of the assessment. The team will also define the current state of the system’s security and develop suggestions for additional security requirements as appropriate. The team’s ultimate goal is to produce a working document in the form of a risk analysis that will assist management in allocating appropriate resources. Appendix D shows examples of the key personnel who should support and participate in the risk analysis and management process.

In addition, the team should use a combination of the following information gathering techniques to collect information relevant to the IT system within its operational boundary. These techniques can be used in all phases of the risk analysis process.

* Questionnaire - Develop a questionnaire concerning the management and operational controls planned for the system. Distribute the questionnaire to the applicable technical and non-technical management personnel who are designing or supporting the IT system.
* **On-Site Interviews**: Interviews with IT system support and management personnel can assist the risk analysis team in collecting useful information about how the IT system is operated and managed. It can also allow the gathering of information from observation about the physical, environmental, and operational security of IT systems. [NIST SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) contains sample interview questions.
* **Document Review**: The RA team should review policy documents (such as legislative, regulatory directives, and organizational policy), system documentation (such as user guides, system administration manuals, system design, and requirements documents, and acquisition documents) and security related documentation (such as system security plan, audit reports, previous RAs, security policy, and security test results), which will help identify required controls as well as those protective measures already in place or planned for the system. The agency’s mission impact analysis or asset criticality assessment will provide information regarding system and information criticality and sensitivity.

* **Automated Scanning Tools**: Scanning tools provide technical information about the system and may also identify risks not yet remediated. These tools are discussed in depth in Section 5.0.

Details of each of the risk activities can be found in [NIST SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) . Figure 1, below, is an illustration of NIST identified risk analysis activities, which will be covered in subsequent sections of this document:



Figure . Risk analysis methodology

#

# Introduction

## Purpose

This document helps facilities identify known threats and vulnerabilities that may apply to IT systems and to the facility’s physical and environmental controls. This list of threats and vulnerabilities does not produce complete listing, and assessors should consider all potential threats to patient data. The document also helps assessors to

* evaluate the likelihood that an identified vulnerability can be exploited
* assess the effects associated with these threats and vulnerabilities
* identify the overall risk level

This RA is intended to leverage <INSERT COMPANY’S NAME HERE> automated tools to enhance IT security across <INSERT COMPANY’S NAME HERE>. An automated approach will also reduce the burden and effort required of IT support staff in the field.

## Scope

The local IT systems are part of a larger infrastructure managed by <INSERT COMPANY’S NAME HERE>. This RA is focused on local electronic health record systems, overarching IT assets and the facility’s physical/environmental controls that may affect the integrity and availability of critical health care systems.

This risk analysis includes the potential risks to and vulnerabilities of the confidentiality, integrity, and availability (CIA) of all of the facility’s created, received, maintained, or transmitted electronic Patient Health Information (e-PHI). Risks to IT systems should beevaluated in the managerial, operational, and technical security domains as defined in FIPS-200, [*Minimum Security Requirements for Federal Information and Information Systems*](http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf) and NIST SP 800-53, Rev 3, <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf>.

This report documents the findings and appropriate controls implemented at the local <INSERT COMPANY’S NAME HERE> facility and will assist management in understanding the security posture of both local and interconnected IT systems across <INSERT COMPANY’S NAME HERE>. This RA is ongoing and should be updated on a continuous basis. The ongoing analysis of findings will be attached in the appropriate Appendices to this document.

## System Characterization

Characterizing an IT system establishes the scope of the risk analysis effort and provides information essential to safeguarding Agency resources. This section helps you identify the boundaries of the IT system and the resources and information that constitute the system.

Characterizing systems includes reviewing system documentation and conducting interviews to gather critical information n. The information collected in Table 1, below, is used to gain an overall understanding of the ownership and functionality of the local IT resources**.** This table may have to be modified to reflect the local environment as appropriate.

Table 1. IT System Inventory and Definition Document

| **IT System Inventory and Definition Document** |
| --- |
| **I. IT System Identification and Ownership** |
| **IT System Name** | List the names of all systems in this location. |
| **Facility Name & Location** |  |

| **IT System Inventory and Definition Document** |
| --- |
| **I. IT System Identification and Ownership, Continued** |
| **IT Systems Overview** | A short detailed summary describing each of the systems listed under IT System Names should be given here.  |

| **IT System Inventory and Definition Document** |
| --- |
| **I. IT System Identification and Ownership, Continued** |
| **RA Team Members** **(if team approach utilized)** |  |  **Phone Numbers** **(list each phone number)** |  |
| **II. IT System Boundary and Components** |
| **Description of IT Systems and Components** | (Attach a copy of the local inventory from Network Scans in Appendix B) |
| **System Interfaces** | All IT access to facility resources is limited to internal <INSERT COMPANY’S NAME HERE> connections or is approved through an Interconnection Security Agreement. Yes [ ]  No [ ]  **(IF NO - All external connections are prohibited to facility resources unless the connections are approved and documented in Section III below and on file with the <INSERT COMPANY’S NAME HERE> facility)** |
| **IT System Boundary** | (Attach a network diagram in Appendix A showing all external connections into the local facility’s internal network) |
| **III. IT System Interconnections** |
| **Agency or Organization** | **IT System Name** | **IT System Owner** | **ISA Status** |
| ***Provide details of any external connections to facility resources if an Interconnection Security Agreement (ISA) has not been executed. No entry needed if Agreements are already on file.***  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **IT Sensitivity Rating and Classification** | The security category of the IT system is determined based upon the impact to confidentiality, integrity, and availability of all system data, specified by [FIPS-199](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf). Based on storage and access to patient data, all <INSERT COMPANY’S NAME HERE> facilities are categorized at a Sensitivity Rating of **High** and a Classification of **Sensitive**. |

## Network Architecture Diagram

Insert a diagram or provide a description of the overarching network architecture in Appendix A. This should include all routers, switches, servers and other devices that contain, transmit, or receive patient data or other sensitive information. This must also include communications links to your facility, for example, outside connections to <INSERT COMPANY’S NAME HERE>, Internet service providers or vendors. If the facility does not have a network architecture diagram, the following tools can help the facility create one:

* [Microsoft Visio](http://office.microsoft.com/en-us/visio/)
* [The Dude Network Monitor](http://www.mikrotik.com/thedude.php) (free)
* [Solar Winds LAN Surveyor](http://www.solarwinds.com/products/lansurveyor/)

Note that the IHS Division of Information Security may not approve the use of specific software packages on IHS systems.

#

# Threat Identification

A threat is the potential for a particular threat source to accidentally trigger or intentionally exploit a specific vulnerability. A threat source is defined as any circumstance or event that could harm an IT system. The threat sources can be natural, human, or environmental. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat source does not present a risk when no vulnerability can be exercised. In determining the likelihood of a threat, consider threat sources, potential vulnerabilities, and existing controls.

This section helps the assessors evaluate the potential for a threat to successfully trigger or exploit a vulnerability and the impact to the facility. It also helps to identify a corresponding response using a hazard-specific scale. In assessing threats, assessors must consider all potential threat sources that could cause harm to the IT systems, the processing environment and potentially the network. In the following pages, common threats have already been listed. These have been listed regardless of their likelihood, geographic impact, or potential outcome. You can add or delete items that don’t apply in the facility’s geographical area. For example, if the facility is located in the desert, you can remove hurricane because of the low likelihood of such an event occurring. Likewise, other items can be added that are specific to the geographical area. The goal is develop a comprehensive, relevant list for the local internal and external environment.

**Instructions for included spreadsheet:** In the following pages a spreadsheet has been inserted. Double -click the spreadsheet to enter your answers. Select 0, 1, 2, or 3 for each category. The Risk column automatically calculates your risks based on the probability and impact. In determining your answer, the issues listed in Table 2, below, should be considered. As you are answering the questions, assume each threat source occurs at the worst possible time (for example, during peak patient loads). For more details on threat and vulnerability identification, refer to [NIST SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) and [NIST SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf).

Table . Considerations for Determining Threat Potential

|  |  |
| --- | --- |
| Issues to consider for **probability (likelihood)** include, but are not limited to:* Known risk
* Historical data
* Manufacturer/vendor statistics
* Incident reports
* Security Reports
* Information gathering
 | Issues to consider for **human impact** include, but are not limited to: * Potential for staff death or injury
* Potential for patient death or injury (includes visitors)
 |
| Issues to consider for **property impact** include, but are not limited to: * Cost to replace
* Cost to set up temporary replacement
* Cost to repair
* Time to recover
 | Issues to consider for **service impact** include, but are not limited to: * Service interruption
* Employees unable to report to work
* Customers unable to reach facility
* Facility in violation of contractual agreements
* Imposition of fines and penalties or legal costs
* Interruption of critical supplies
* Interruption of product distribution
* Reputation and public image
* Financial impact/burden
* Violation of federal mandates
 |
| Issues to consider for **preparedness** include, but are not limited to: * Status of current emergency plans
* Frequency of drills
* Training status
* Availability of alternate sources for critical supplies/services
 | Issues to consider for emergency **response** include, but are not limited to: * Time to marshal an on-scene response
* Scope of response capability
* Historical evaluation of response success
 |





# Vulnerability Identification

This section provides information for developing a list of system vulnerabilities that could be exploited and contains tools to help facilities identify technical vulnerabilities.

If a facility chooses not to use one of the tools in this section, it can be deleted. And if a facility has other tools to identify vulnerabilities, they can add sections. The facility should also catalog other vulnerabilities as part of the identification process that could result in a security breach or a violation of a system security policy. The following list provides examples of vulnerabilities that the automated tools might not identify are:

* Social engineering of users, the help desk, or the user support team
* Misconfiguration of hardware, software or operating system
* Terminated employee accounts not removed from the system
* Water sprinklers to suppress fire in a data center
* Controls/measures not in place to physically protect equipment and information

## Network Scans <List the Tool(s) Used> – (Continuous Monitoring/Monthly Reports)

**DESCRIPTION:** Network scans can search for security configuration compliance and vulnerability compliance. Security Content Automation Protocol (SCAP)-compliant scans can help the facility create asset inventories, and enterprise-wide reports on security vulnerabilities and configuration compliance. Network scans could fully automate an enterprise-wide measurement and reporting of compliance with the <INSERT COMPANY’S NAME HERE> system standards, for example, the federal government uses the Federal Desktop Core Configuration (FDCC) standard and the United States Government Configuration Baseline (USGCB).

Network scans can contribute the following types of information:

* Asset Discovery: Rapidly discovers and inventories all networks and network assets, including managed and unmanaged devices,
* Configuration Management: Maintains an accurate inventory of system configurations, including technical controls, software, user accounts and system changes,
* Vulnerability Management: Conducts ongoing vulnerability detection and reporting for operating systems, infrastructure, network applications and databases, and
* Policy Management: Continuously evaluates system configuration for compliance with organizationally defined standards and policies.

The four functions highlighted above can continuously funnel information into a centralized portal. As a result, the streamlined, automated, and end-to-end measurement process can more accurately measure and ensure compliance with many federal mandates, including FDCC, USGCB and [NIST SP 800 -53, Rev 3](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf).

**Example rating scale and input for RA:** Vulnerability scans are conducted continuously with monthly reports of findings provided to management. Management must work with appropriate personnel towards mitigating existing and new vulnerabilities on a continual basis. The grading scale is shown below in Table 3. **Failure to maintain adequate scoring metrics may result in decertification for MU and/or authorization to operate IT systems at your facility. Other actions may be taken as appropriate based upon severity or risk to <INSERT COMPANY’S NAME HERE> resources.**

Table . Grading scale for High Risk Aging and Mitigation

|  |  |  |
| --- | --- | --- |
| **High Risk Aging** |  | **High Risk Mitigation** |
| < 30 days | A+ |  | 80 - 100% | A+ |
| 31-45 days | A |  | 70 - 79% | A |
| 46-60 days | B |  | 60 - 69% | B |
| 61-75 days | C |  | 50 - 59% | C |
| 76-90 days | D |  | 40 - 49% | D |
| > 90 days | F |  | < 40% | F |

Vulnerability findings and copies of approved mitigation plans should be attached in the Appendix. An example mitigation plan is included as Appendix E.

## Penetration Testing – (Performed Annually)

**DESCRIPTION** Penetration testing is a way to evaluate the security of computer systems and networks by simulating an attack from a malicious source. <INSERT COMPANY’S NAME HERE> has established a penetration testing program as part of the <INSERT COMPANY’S NAME HERE> cybersecurity plan. The program seeks to simulate malicious attacks from both inside and outside the facility. Penetration testing, when used in risk analysis, can be used to assess an IT system’s ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat source, identify potential failures and vulnerabilities in the IT system protection schemes, and provide IT staff with recommendations to address each security risk.

The findings of the penetration test detail the approach, methodology, procedures, and results of the test. The facility will receive a written report, which should include high-, medium-, and low-risk findings. Each finding should also include the following information:

* Description
* Affected Hosts
* Impact
* Recommendation
* Sources for Corrective Action

**INPUT for RA:** Penetration test reports and mitigation plans or mitigation progress reports should be attached in the appendix.

## Intrusion Prevention System – <List Tools Used> (Continuous Monitoring)

**DESCRIPTION:** An intrusion prevention system (IPS) looks for malicious and unwanted traffic to detect attacks (worms, viruses, Trojans, blended threats, Phishing, Spyware, VoIP Threats, DoS, DDoS, Backdoors, Walk-in Worms, Bandwidth Hijacking) before damage occurs. IPSs address many compliance program objectives including vulnerability management and network monitoring and provide automated enforcement of network security policies.

**INPUT to RA:** IPSs often have the flexibility to create a variety of customizable reports. Insert any findings and corresponding information in the Appendix.

## Wireless Site Survey Tools – (Performed Annually)

**DESCRIPTION:** Wireless site survey tools provide a visualization of wireless devices transmitting within a facility. They can identify signal interference with medical devices, reveal areas with weak or nonexistent coverage, discover the existence and location of rogue access points, and map signals that leak out of a facility into the public domain. For sites without wireless, site surveys can detect rogue wireless networks within their facility.

**INPUT to RA:** Site survey reports and mitigation plans or progress reports should be attached as an appendix.

## Malware Detection – <List Tools Used> (Continuous Monitoring)

**DESCRIPTION:** Some malware detection software can find zero-day malware that uses network exploits to attack the network and automatically capture that malware for analysis and response. With such evidence, IT professionals can dig deep into threats and conduct forensic analysis to effectively characterize and respond to malware in the way that is most effective for an organization.

## Log Management – <List Tools Used> Periodic Review of Logs)

**DESCRIPTION:** Some log management tools include search capabilities that enable you to view and analyze system activity and provide evidence of various system activities. Log management tools should support collection of raw or unstructured logs, Syslog, Common Event Format, and other file-based log sources.

## Other Tools

Your facility may have access to other security tools that are not included in this template. The combination of tools can significantly enhance a facility’s’ security posture and decrease potential risk. Add appendices to accommodate additional reporting tools.

#

# Control Analysis

Control analysis evaluates the controls that the organization has implemented or plans to implement in order to minimize or eliminate the risks identified in the risk analysis. By implementing security controls, the level of risk to the IT systems and data will be reduced to an acceptable level.

To determine which security controls are required and appropriate, the facility can conduct a cost-benefit analysis for any planned controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level or risk. In addition, the effect on system performance and feasibility (for example, technical requirements, user acceptance) of introducing the planned controls should be evaluated carefully during this process.

**IMPORTANT**: Using [NIST SP 800-53, Rev 3](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf) as a checklist can help facilities analyze security controls efficiently and systematically. Some of the major controls are listed in Table 4 below. However, facilities must modify and update the table to accurately reflect its IT environment.

Table . Security Controls Checklist

| Control Area | Description of Controls |
| --- | --- |
| **1 Risk Management** |
| **1.1 IT Security Roles & Responsibilities** | ***List the name, title, and role for each employee with facility IT security responsibilities.***  |
|  |
| **1.2 IT policy and Procedure** | ***List the facility IT security related policies and/or procedures*** |
| ***[ ] Abide by or have adopted <INSERT COMPANY’S NAME HERE> policies and procedures******[ ] Other (Provide details)*** |
| **1.3 IT System & Data Sensitivity Classification** | ***Provide the classification of data per FIPS-199*** |
| ***[ ] High******[ ] Moderate******[ ] Low*** |
| **1.4 IT System Inventory** | ***Explain how the IT systems are inventoried and if the inventory is current*** |
| ***[ ] Utilizing Network scans for inventory******[ ] Utilizing a combination of Network scans and others******[ ] Other (Provide details)*** |
| **1.5 IT Security Audits** | ***List and describe any IT security audits (such as an <INSERT COMPANY’S NAME HERE> Penetration Test)*** |
| ***[ ] Adopted security audits as described in Section 5******[ ] Other (Provide details)*** |
| **2 IT Contingency Planning** |
| **2.1 Continuity of Operations Planning** | ***Discuss the COOP plan for the facility (A template is available from OIT upon request – POC:<insert contact information>*** |
| ***[ ] COOP Plan complete and alternate facility available******[ ] COOP Plan complete but no alternate facility available******[ ] No COOP Plan in place******[ ] Other (Provide details)*** |
| **2.2 IT Disaster Recovery Planning** | ***Discuss the IT Disaster Recovery Plan (May be part of the overall IT COOP Plan)*** |
| ***[ ] Already included in COOP Plan******[ ] Other (Provide details)*** |
| **2.3 IT System & Data Backup & Restoration** | ***Discuss the Data Backup and Restoration process for IT systems*** |
| ***[ ] Already included in COOP Plan******[ ] Data backup and restoration addressed separately******[ ] Other (Provide details)*** |
| **3 IT Systems Security** |
| **3.1 IT System Hardening** | ***Discuss IT system hardening such as configuration settings, patch level, Service Packs, Firewalls, etc.*** |
| ***[ ] System hardening is enforced through Group Policy******[ ] Other (Provide details)*** |
| **3.2 Malicious Code Protection** | ***Discuss Anti-Virus software products in use*** |
| ***[ ] Utilizing Antivirus X******[ ] Utilizing Antivirus Y******[ ] Other (Provide details)*** |
| **4 Logical Access Control** |
| **4.1 Account Management** | ***Discuss how User Accounts are managed and controlled*** |
| ***[ ] Abide by or have adopted <INSERT COMPANY’S NAME HERE> policy******[ ] Other (Provide details)*** |
| **4.2 Password Management** | ***Discuss Password Requirements*** |
| ***[ ] Abide by or have adopted <INSERT COMPANY’S NAME HERE> policy******[ ] Other (Provide details)*** |
| **4.3 Remote Access** | ***Discuss how remote access is utilized at the facility.*** |
| ***[ ] Utilizing VPN solution X******[ ] Utilizing VPN solution Y******[ ] Other (Provide details)*** |
| **4.4 Separation of Duties** | ***Discuss how the concept of separation of duties is enforced to ensure that no single individual has control of the entirety of a critical IT processes.*** |
| ***[ ] Abide by or have adopted policies covered under <Insert name of company policy>******[ ] Other (Provide details)*** |
| **5 Data Protection** |
| **5.1 Data Storage Media Protection** | ***Discuss how portable media and mobile devices are controlled and the data stored on those devices is protected*** |
| ***[ ] Utilizing XX protection for removable media******[ ] Other (Provide details)*** |
| **5.2 Encryption** | ***Discuss the encryption being utilized on IT devices (select all that apply)*** |
| ***[ ] Utilizing A for encryption of data in transit******[ ] Utilizing Y for full disk encryption******[ ] Other (Provide details)*** |
| **6 Facilities Security** |
| **6.1 Facilities Security** | ***Discuss physical security of the facility*** |
| ***[ ] Physical access is controlled through employee badges and visitor sign-in.******[ ] Other (Provide details)*** |
| **6.2 Power** | ***Discuss controls to ensure power to critical IT systems is maintained during an outage (select all that apply)*** |
| ***[ ] Critical IT systems are supported by UPS******[ ] Critical IT systems are supported by a generator******[ ] Other (Provide details)*** |
| **6.3 Restricted Areas** | ***Discuss how restricted areas such as the “computer room” or “data center” are secured*** |
| ***[ ] Rooms are secured with limited access******[ ] Rooms are unsecured but access is monitored******[ ] Other (Provide details)*** |
| **6.4 Temperature and Humidity** | ***Discuss how Temperature and Humidity are controlled*** |
| ***[ ] Temperature and humidity are controlled through the facility HVAC******[ ] Other (Provide details)*** |
| **7 Personnel Security** |
| **7.1 Access Determination & Control** | ***Discuss how an employee gains access to the facility, restricted areas, and IT systems. Discuss what determines the level of access they receive. Discuss how and when access is removed (Select all that apply)*** |
| ***[ ] <INSERT COMPANY’S NAME HERE> issued Smartcard, Bio-metric, or token authentication are utilized for physical access******[ ] <INSERT COMPANY’S NAME HERE> issued Smartcard, Bio-metric, or token authentication are utilized for logical/logon to IT systems******[ ] Removal of access to <INSERT COMPANY’S NAME HERE> resources is addressed through <INSERT COMPANY’S NAME HERE> policy*** ***[ ] Other (Provide details)*** |
| **7.2 IT Security Awareness & Training** | ***Discuss the IT Security Awareness and Training employees are required to participate in*** |
| ***[ ] Employees and contractors take <INSERT COMPANY’S NAME HERE>’s annual security awareness training******[ ] Other (Provide details)*** |
| **7.3 Acceptable Use** | ***Discuss the Acceptable Use policy*** |
| ***[ ] Abide by or have adopted <INSERT COMPANY’S NAME HERE> policy as described in the <INSERT COMPANY’S NAME HERE> Rules of Behavior and <INSERT COMPANY’S NAME HERE> Manual******[ ] Other (Provide details)*** |
| **8 Threat Management** |
| **8.1 Threat Detection** | ***Discuss how IT threats are detected*** |
| ***[ ] Utilizing <INSERT NAME OF SECURITY TOOL> tools as described in Section 5******[ ] Other (Provide details)*** |
| **8.2 Incident Handling** | ***Discuss how IT incidents are handled*** |
| ***[ ] Incidents are reported to the appropriate Incident Response personnel*** ***[ ] Other (Provide details)*** |
| **8.3 Security Monitoring & Logging** | ***Discuss how security is monitored and the logging capabilities of IT systems*** |
| ***[ ] Utilizing <INSERT NAME OF SECURITY TOOL> tools as described in Section 5******[ ] Other (Provide details)*** |
| **9 IT Asset Management** |
| **9.1 IT Asset Control** | ***Discuss how computers are controlled. Such as leaving the premises, connected to the network, disposal, etc.*** |
| ***[ ] IT systems are controlled through the use of property receipts******[ ] Other (Provide details)*** |
| **9.2 Software License Management** | ***Discuss the software policy (select all that apply)*** |
| ***[ ] Applications are identified and tracked through network scans******[ ] Licensing is tracked manually******[ ] Abide by or have adopted <INSERT COMPANY’S NAME HERE> policies******[ ] Other (Provide details)*** |
| **9.3 Configuration Management & Change Control** | ***Discuss how configuration management and change control is handled*** |
| ***[ ] Utilizing the <INSERT COMPANY’S NAME HERE> change control processes******[ ] Utilizing a ticketing system to manage and track system changes******[ ] Other (Provide details)*** |
| **10 Other** |
| **10.1 Other** | ***Add rows as needed to document additional security controls as described in*** [***NIST (SP) 800-53, Rev 3***](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)***.***  |
|  |

#

# Risk Mitigation Strategies

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk analysis. Because eliminating all risk is usually impractical or close to impossible, senior management and functional and business managers must use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization’s resources. It may not be practical to address all identified risks, so priority should be given to the threats and vulnerabilities with the potential to cause significant harm to mission or people.

Appendix E contains a template for documenting risks and provides for recommended controls for senior management approval. Instructions are provided on the Risk Mitigation Worksheet. This template will be used for findings identified through penetration testing, wireless surveys or other IT security tools. Many of the details of this plan, such as the device information, list of individual vulnerabilities, and the point of contact information, are automatically generated. The only fields a facility is required to manually complete are the device description, mitigation plan, removal impact, estimated cost and a planned remediation date.

# Appendix A: Network Diagram(s)

# Appendix B: Monthly Network Scan Reports

Annual Inventory

Year One

|  |
| --- |
|  |

|  |
| --- |
|  |

Facility Evaluated: Date:

# Appendix C: Annual Penetration Test

# Appendix D: Key Roles in a Risk Assessment

Table 5 shows examples of the key personnel who support and participate in the risk analysis and management processes. For detailed description of specific roles and additional roles for the Risk Management Framework, please refer to NIST SP 800-30, which can be found at [http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\_30\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf), and NIST SP 800-37, <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.

Table . Roles and Responsibilities

| Role | Responsibility |
| --- | --- |
| Senior Management | Under the standard of due care and ultimate responsibility for mission accomplishment, must ensure the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of risk analysis activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management. |
| Information Technology Director or Chief Information Officer (CIO) | Responsible for the facility’s IT planning, budgeting, and performance, including its information security components and compliance. Decisions made in these areas should be based on effective risk management program. |
| System and Information Owners | Responsible for ensuring proper controls are in place to address integrity, confidentiality and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems (for example, system enhancements, major changes to the software and hardware). Therefore, they must understand their role in the risk management process and fully support this process. |
| Business and Functional Managers | Responsible for business operations and IT procurement process and must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources. |
| Chief Information Security Officer (CISO)/Information Systems Security Officer (ISSO) | IT security program managers and computer security officers are responsible for their organizations’ security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations missions. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis. |
| IT Security Practitioners | IT security practitioners (for example, network, system, application, and database administrators, computer specialists, security analysts, security consultants, developers) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT environment (for example, expansion in network connectivity, changes to existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems. |

# Appendix E: Risk Mitigation Worksheet

(Instructions: This worksheet is designed to document how you are going to handle each of the risks identified during the risk analysis process. If you identified twenty (20) risks you would have twenty (20) worksheets. The RA Team should work together to complete the worksheets. The Facility Director or designee will evaluate the selections and agree to each (e.g., accepting the risks and chosen recommended controls) or will negotiate an alternative mitigation strategy.

Date Completed:

Date Last Modified:

**Certifying Authority Signature: Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| **Risk #** | **Risk****(High/Moderate/Low)** | **Risk Statement** |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Recommendations | Implement Recommendation? Y/N | Proposed Alternatives | Response/Comments |
|  |  |  |  |

**Recommendation That Risk Be Accepted As Mitigated**

 **Certifying Authority Initials:**

 **Comments:**

# Security Review and Attestation

Initial Year

Both parties agree that adequate and acceptable IT security measures are in-place to protect <INSERT COMPANY’S NAME HERE>/ resources under the local control of the facility identified on the cover of this Risk Analysis.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | **Signature of Facility IT Director ate** |
|  |  |  |
|  |  |  |
|  |  | **Signature of <Company CEO> Date** |