

Department of Veterans Affairs



SMART-RiskWatch

Reference Guide

Version 1.1

October 2007

FOR OFFICIAL USE ONLY

Table of Contents

<u>Introduction.....</u>	1
<u>Chapter 1 ✧ Let's Conduct a Risk Assessment.....</u>	2
<u> Objectives.....</u>	2
<u> Starting Your Risk Assessment In SMART.....</u>	2
<u> Risk Watch Terminology</u>	4
<u>Chapter 2 ✧ Entering and Editing Data.....</u>	5
<u> Objectives.....</u>	5
<u> Company Data</u>	5
<u> Add and Edit Assets.....</u>	5
<u> Selecting Safeguard</u>	6
<u> Threat Frequencies.....</u>	7
<u>Chapter 3 ✧ Reports.....</u>	8
<u> Objectives.....</u>	8
<u> Ancillary Reports.....</u>	8
<u> Response Analysis Report</u>	9
<u> Introduction Report.....</u>	11
<u> Executive Summary.....</u>	11
<u> Recommendations Report.....</u>	11
<u> Full Asset Report.....</u>	12
<u> Summary by Asset Report</u>	12
<u> Full Threat Report.....</u>	12
<u> Summary by Threat Report.....</u>	12
<u> Full Vulnerability Report.....</u>	13
<u> Full Safeguard Report.....</u>	13
<u> Cost Benefit Report.....</u>	13
<u> Safeguard Threat Report.....</u>	14
<u> Appendix A – Things to Do Before Starting a Risk Assessment.....</u>	14
<u> Appendix B – Risk Assessment Asset List and Example of Asset Costs for 3000 employees</u>	15
<u> Appendix C – Glossary of Safeguards</u>	16

Introduction

SMART Division has taken RiskWatch® and integrated in SMART. This makes creating a risk assessment easy. It allows you to quickly create a sharp, professional risk management plan. This manual has been written to assist you in getting the most out of SMART/RiskWatch® integration.

Each chapter in this manual will guide you through a set of related features in SMART to create a risk assessment. Chapters begin with objectives and include a series of screens to show you what to expect when clicking on an item.

There is a help feature, if you need assistance. Suggestions for improvements to this manual, and all comments, are always welcome. Please send them to Kitty Koepping via e-mail at kitty.koepping@mail.va.gov or call 304-262-7731. Enjoy creating a risk assessment.

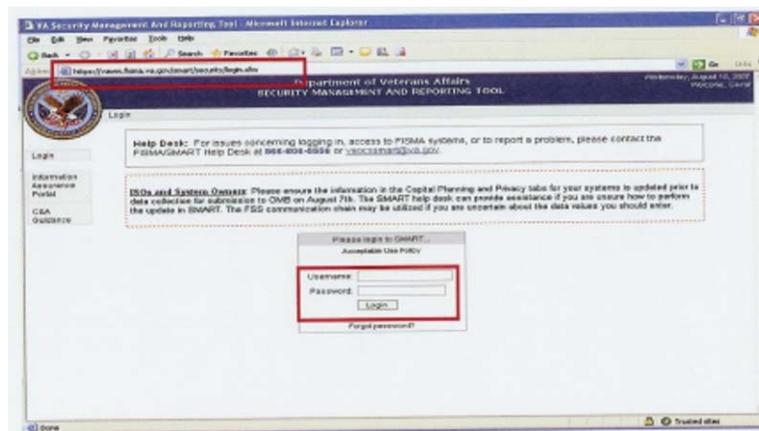
Chapter 1 ✦ Let's Conduct a Risk Assessment

Objectives

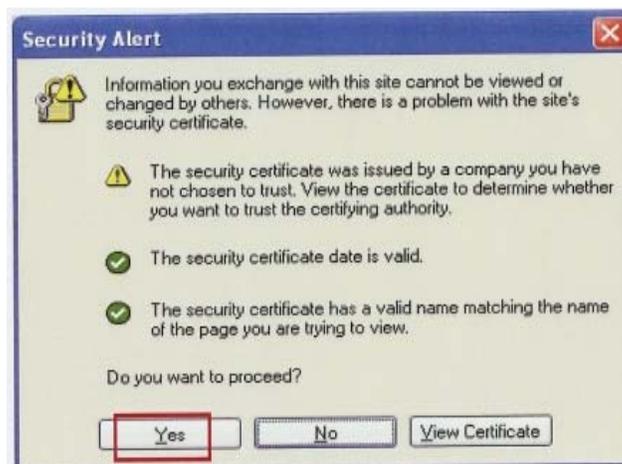
Starting the Risk Assessment Portion of SMART
Understand Risk Assessment Terminology

Starting Your Risk Assessment In SMART

SMART database is now on a web site. Using Internet Explorer log on to <https://vaww.fisma.va.gov/smart>. This logs you into the SMART database. If you do not have access, call the SMART help desk at 866-806-5556 and request a password to the database. Type in your **Username** and **Password** then select "Login".



When you log into this URL a Security Alert screen appears. Select "Yes".



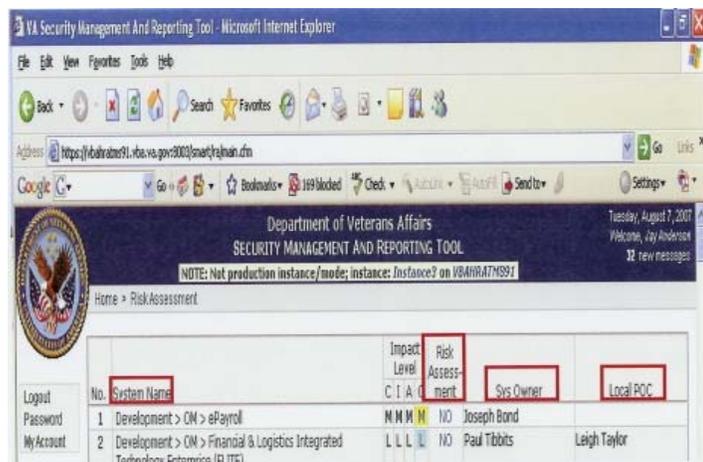
Risk Assessment Using SMART Reference Guide Version 1.0

October 2007

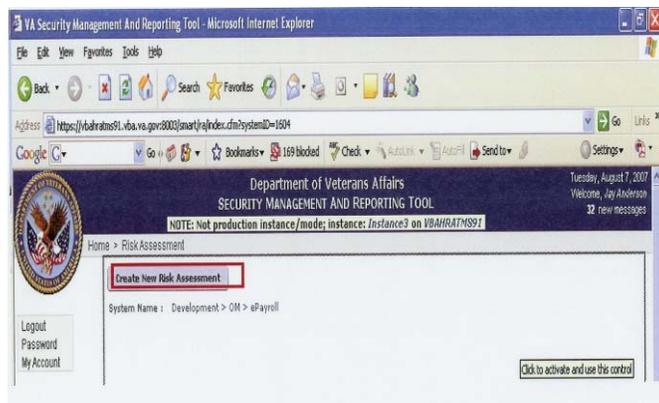
Select the “**Risk Assessment**”. This will bring up all systems in SMART.



Select your **system** you need to do a risk assessment on. You can check if you have a **risk assessment** on file, who the **system owner** is, and the **local POC**.



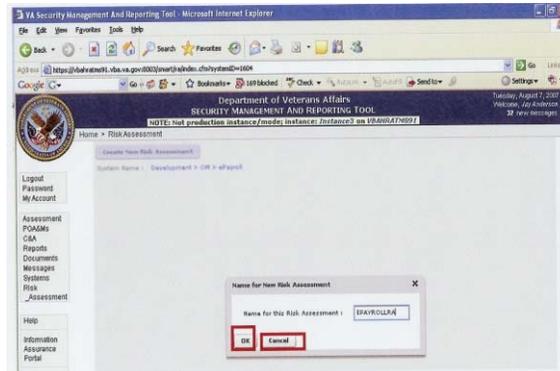
Select the ‘**Create New Risk Assessment**’ button.



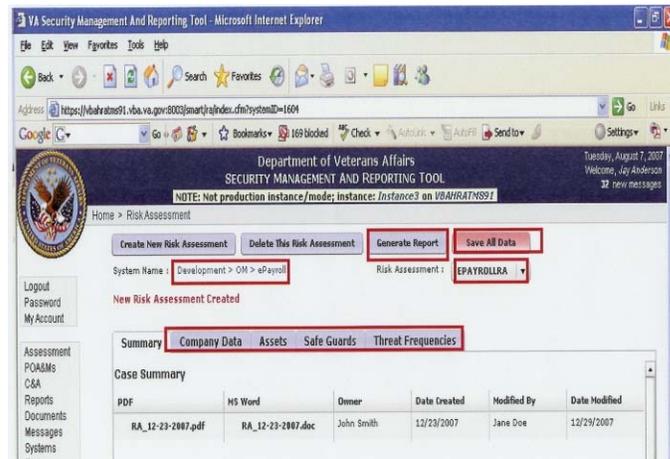
Risk Assessment Using SMART Reference Guide Version 1.0

October 2007

You will be prompted to name the risk assessment. Usually you will type the name of the system (i.e., **ePayroll RA**). This designates this risk assessment belong to this system. Then click on **“OK”**.



This screen shows that you can **delete** this risk assessment, **generate a report**, **save all data**, and the **name** of this risk assessment. There are several tabs on this screen. The “Summary” tab shows all the reports that are available. **“Company Data”**, **“Assets”**, **“Safe Guards”**, and **“Threat Frequencies”** are all tabs you need to fill out information in to fill out the risk assessment.



Risk Assessment Terminology

In order to effectively use the Risk Assessment portion of the SMART database, it is important to be comfortable with the following terms.

Asset Categories – the different assets (i.e., servers, pcs, financial information, etc.) in your facility.

Threats – the threats associated with your facility, its locality and your environment.

Safeguards – these are the precautions that are in place to protect your assets.

Chapter 2 ✦ Data

Objectives

- Company Data
- Add and Edit Assets
- Selecting Safeguard
- Threat Frequencies

Company Data

You add your facility's name, system to be analyzed with this case, and the value of the mission for your facility. You can have a system, i.e. LAN, and have several sub-assets, such as pcs, servers, firewall, etc.

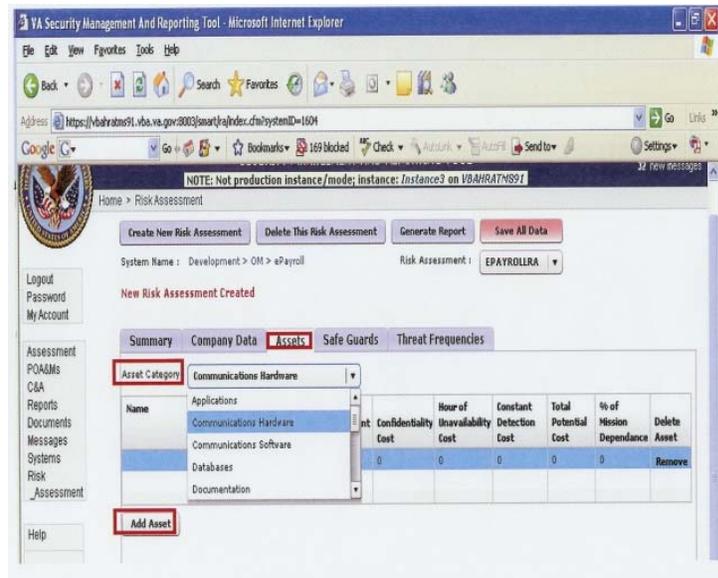
Click on the **"Company Data"** tab. Fill in the screen. Some fields are filled out for you, such as the **Organization Name**. Others you have fill out. Every field is required even if you only put in a zero.

The screenshot shows a web browser window titled "VA Security Management And Reporting Tool - Microsoft Internet Explorer". The address bar shows the URL: "https://bahram911.vba.va.gov:8003/smart/qa/index.cfm?systemID=1604". The page content includes a navigation menu on the left with options like "Logout", "Password", "My Account", "Assessment", "POA&Ms", "C&A", "Reports", "Documents", "Messages", "Systems", "Risk", and "Assessment". The main content area has a "New Risk Assessment Created" message and a "Company Data" tab selected. The form fields are as follows:

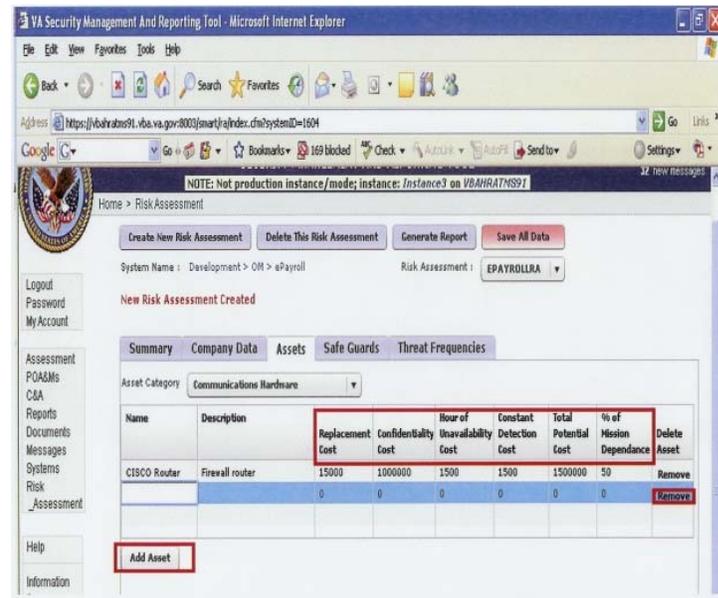
Organization Name :	Office of Management
Number/Code of Organization Unit :	6
Days of Operation per week :	1
Hours of Operation per day :	1
Downtime before serious consequences (hours) :	24
Replacement time for minimal functional support (hours) :	24
Data Sensitivity Level :	Not Applicable
Number of Full-time Users :	160
Maximum \$ system manages (financial systems only) :	0
Yearly mission value for Enterprise :	1000000

Add/Edit Assets

The next click on the **"Assets"** tab. Using the drop down menu of **"Asset Category"**. Select the type of asset you are adding. Select the category and then select the **"Add Asset"** button. This will allow you to add an asset in the **BLUE** row.



Fill in **each cell**. If another asset needs to be added, select “**Add Asset**” again. This will create a new **BLUE** row. If you have added an asset that you no longer have, you can delete the asset, by clicking on the “**Remove**” button.



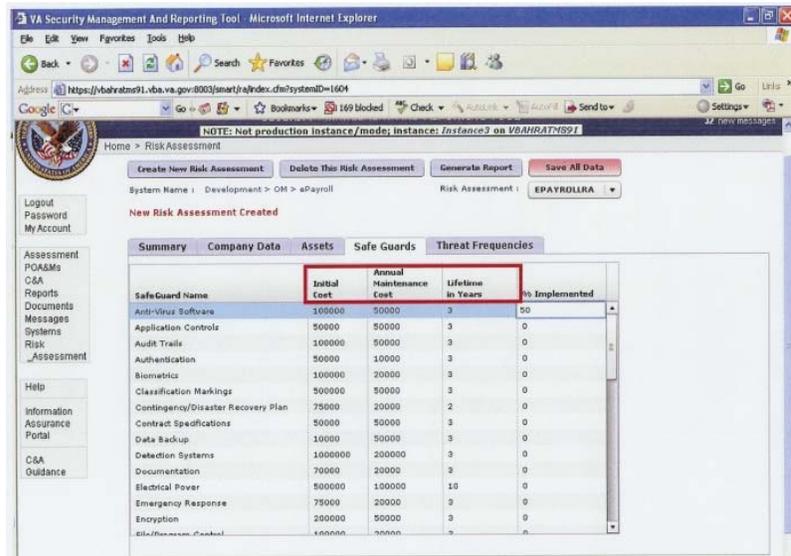
Selecting Safeguards

OCS has filled out the “**Initial Cost**”, “**Annual Maintenance Cost**”, and “**Lifetime in Years**” of each safeguard. These are average costs. If your safeguard cost is higher or lower you can change them, but these are averages throughout the VA. Type in the percentage of the safeguard implemented in the “**% Implemented**” Column. Some of these percentages are from the National level and percentages

Risk Assessment Using SMART Reference Guide Version 1.0

October 2007

will be at 100%, some are at your level and could be as low as “0”. You must fill out every “% Implemented”.

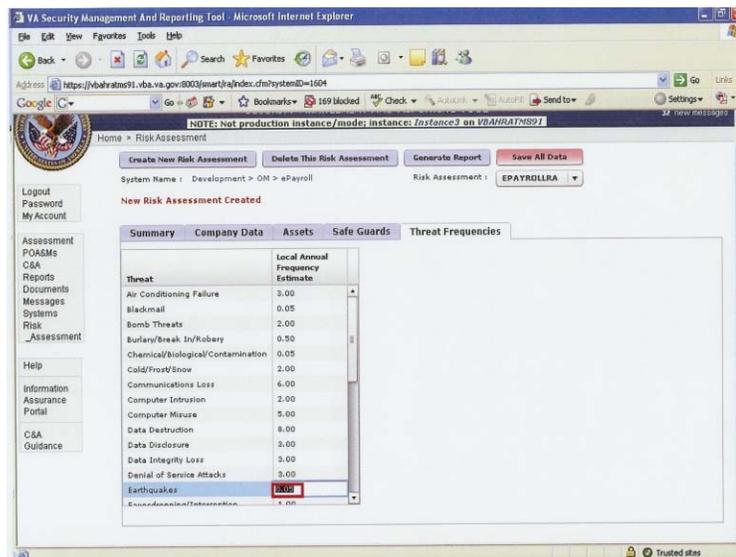


The screenshot shows the VA Security Management And Reporting Tool interface. The main content area displays a table with the following data:

SafeGuard Name	Initial Cost	Annual Maintenance Cost	Lifetime in Years	% Implemented
Anti-Virus Software	100000	50000	3	50
Application Controls	50000	50000	3	0
Audit Trails	100000	50000	3	0
Authentication	50000	10000	3	0
Biometrics	100000	20000	3	0
Classification Markings	500000	50000	3	0
Contingency/Disaster Recovery Plan	75000	20000	2	0
Contract Specifications	50000	50000	3	0
Data Backup	10000	50000	3	0
Detection Systems	1000000	20000	3	0
Documentation	70000	20000	3	0
Electrical Power	500000	100000	10	0
Emergency Response	75000	20000	3	0
Encryption	200000	50000	3	0
File/Process Control	100000	20000	3	0

Threat Frequencies

Threat frequencies are calculated from FEMA’s databases, among other federal databases. But if you live in an **earthquake area**, your threat might be higher, so you can change the frequencies. By researching FEMA’s web site located at www.fema.gov for the frequencies charts will help you to not under or over estimate the frequency.



The screenshot shows the VA Security Management And Reporting Tool interface. The main content area displays a table with the following data:

Threat	Local Annual Frequency Estimate
Air Conditioning Failure	3.00
Blackmail	0.05
Bomb Threats	2.00
Burglary/break In/Robbery	0.50
Chemical/Biological/Contamination	0.05
Cold/Frost/Snow	2.00
Communications Loss	6.00
Computer Intrusion	2.00
Computer Misuse	5.00
Data Destruction	8.00
Data Disclosure	3.00
Data Integrity Loss	3.00
Denial of Service Attacks	3.00
Earthquakes	10.00
Evacuation/Interruption	4.00

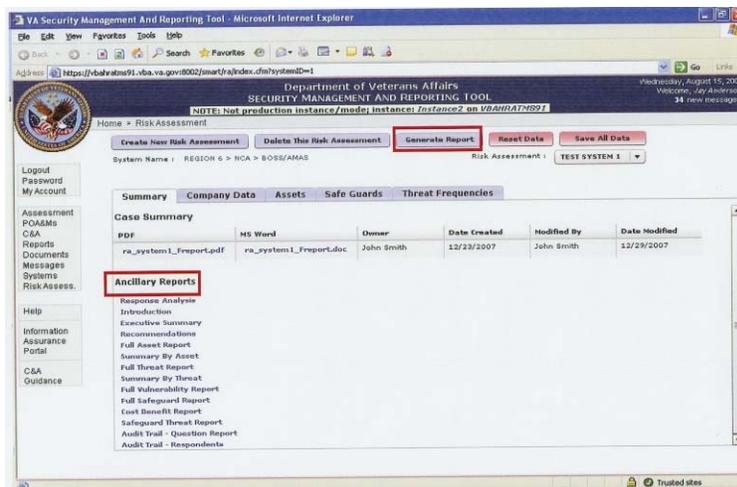
Chapter 3 ✧ Reports

Objectives

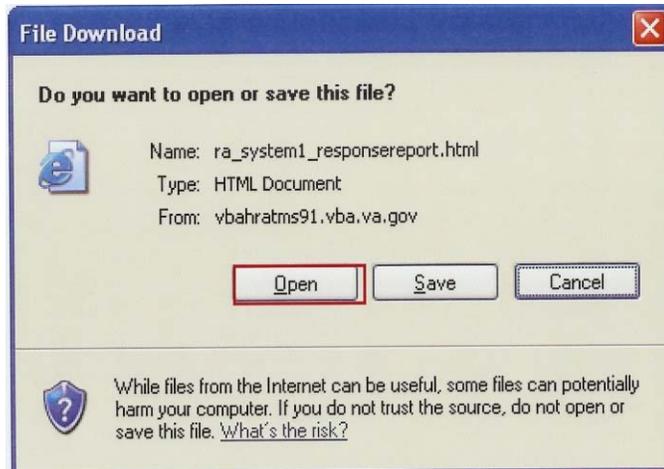
- Ancillary Reports
- Response Analysis Report
- Introduction Report
- Executive Summary
- Recommendations Report
- Full Asset Report
- Summary by Asset Report
- Full Threat Report
- Summary by Threat Report
- Full Vulnerability Report
- Full Safeguard Report
- Cost Benefit Report
- Safeguard Threat Report

Ancillary Reports

To use the reports function, select on the report you want under the “**Ancillary Reports**”. Select the “**Response Analysis**” report or any report.

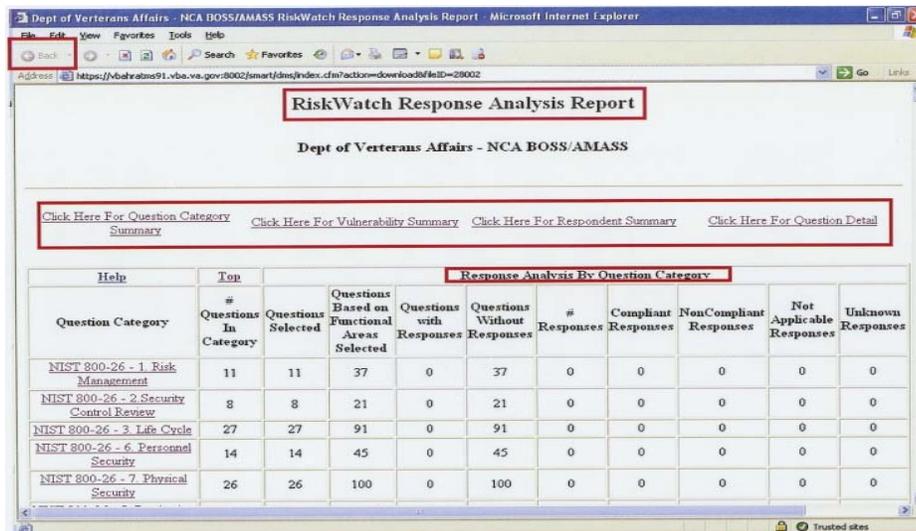


Then the next screen asks you if you want to **open** or save this file. You want to open it.



Response Analysis Report

Opening the first report (**RiskWatch Response Analysis Report**), shows **analysis by Questions category**. You can select any of the options across the top of the report (**Question Category Summary, Vulnerability Summary, Respondent Summary or Question Detail**). The Question Category report is opened by default. Clicking the **"BACK"** button will return you to the default report.



The Vulnerability Summary looks like this:

Response Analysis By Vulnerability										
Vulnerability (Bold indicates selected vulnerability)	# Questions For Vulnerability	# Questions For Selected Vulnerability	Questions Based on Question Categories Selected	Questions Based on Functional Areas Selected	Questions With Responses	Questions With No Responses	#	Compliant Responses	NonCompliant Responses	Not Applicable Responses
Access Control	213	213	213	1138	25	1113	25	11	14	0
Accountability	15	15	15	92	0	92	0	0	0	0
Administration	3	3	3	20	0	20	0	0	0	0
Applications	2	2	2	13	0	13	0	0	0	0
Audit Trails	62	62	62	282	10	272	10	0	10	0
Authentication	59	59	59	280	14	266	14	0	14	0
Communications	68	68	68	322	8	314	8	0	8	0
Compliance	24	24	24	133	0	133	0	0	0	0
Configuration Management	58	58	58	402	5	397	5	0	5	0
Contingency Planning	107	107	107	490	9	481	9	0	9	0
Data Backup/Storage	8	8	8	32	0	32	0	0	0	0
Data Integrity	77	77	77	348	6	342	6	0	6	0
Device & Media Control	48	48	48	212	4	208	4	0	4	0
Disaster Recovery Plan	3	3	3	9	0	9	0	0	0	0
Disclosure	8	8	8	70	0	70	0	0	0	0
Documentation	19	19	19	87	0	87	0	0	0	0
Emergency Incident Response	43	43	43	136	9	127	9	0	9	0

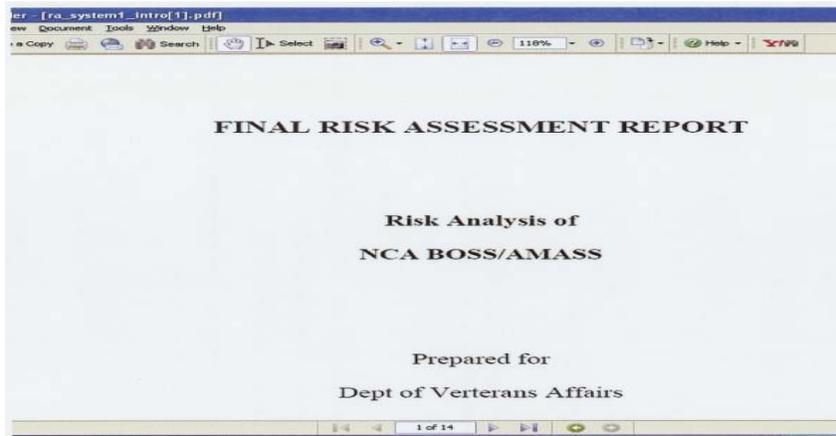
The “Respondent Summary” has what questions were answered by what functional areas.

Response Analysis By Respondent								
Respondent	Functional Areas	# Questions	# Questions w/ Responses	# Responses	Compliant Responses	NonCompliant Responses	Not Applicable Responses	Unknown Responses
MASTER	Accounting Application Software Management Application/Program Security Chief Information Officer (CIO) Chief Security Office (CSO) Chief Technical Officer (CTO) Communications Management Compliance/Legal Database Administration Document and Mag Media Control Financial Management/Budget Help Desk/Technical Support Human Resources/Personnel Services Information Owners Information Security Officer (ISO)	1438	178	178	11	167	0	0

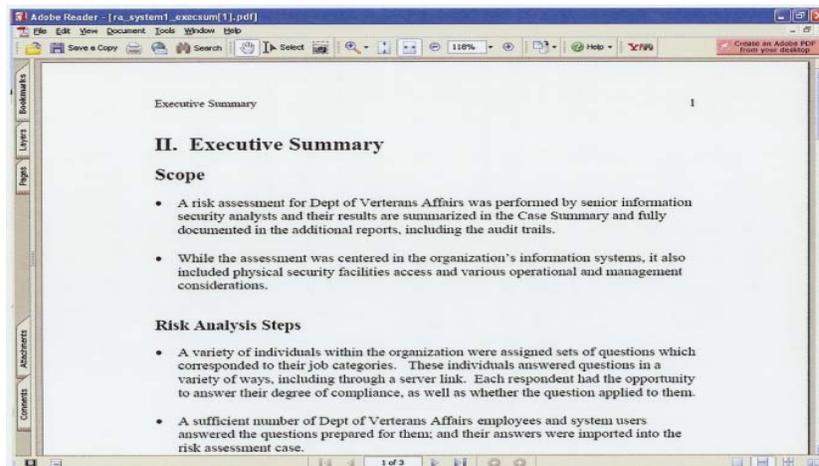
The “Questions Detail” report is a repository of all information, such as the “Control Standard” for each question, what regulation is the **question category** from, the **functional area** who you determined should answer this question and if they **responded** to the question, etc. When opening the reports section, it opens a separate window screen, so to risk return to the list of report, **close** this window.

Question Details						
Question ID	Question Category	Vulnerability Area	Question	Control Standard	Functional Areas	Responses
772	NIST 800-26 - 1 Risk Management	Risk Management Program	Is risk periodically assessed?	Risk should be periodically assessed 1.1 Critical Element - Risk Management	Internal Audit Compliance/Legal Chief Security Officer (CSO) Application/Program Security Chief Information Officer (CIO) Information Security Officer (ISO)	No Responses 11/1
773	NIST 800-26 - 1 Risk Management	Risk Management Program	Is the current system configurations documented, including links to other systems?	The current system configuration should be documented, including links to other systems 1.1.1 NIST SP 800-18	Information Security Officer (ISO) Chief Information Officer (CIO)	No Responses 11/1
774	NIST 800-26 - 1 Risk Management	Risk Management Program	Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?	Risk assessments should be performed and documented on a regular basis or whenever the system, facilities, or other conditions change. 1.1.2 FISACM SP-1	Chief Security Officer (CSO) Compliance/Legal Information Security Officer (ISO)	No Responses 11/1
775					Information Security Officer (ISO)	

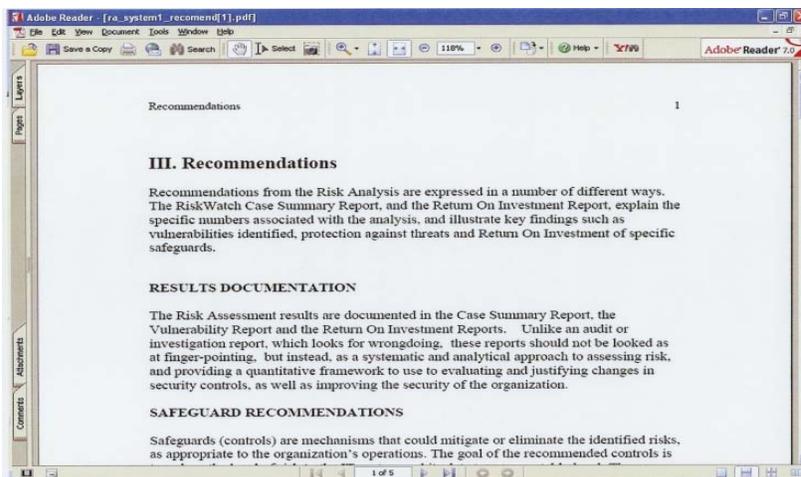
Introduction Report



Executive Summary



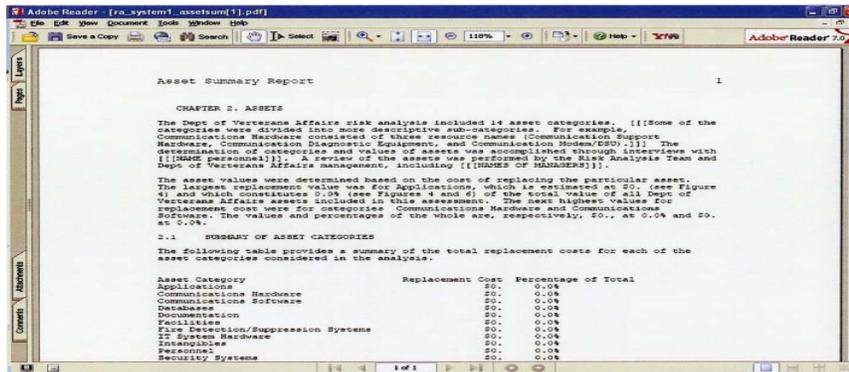
Recommendations Report



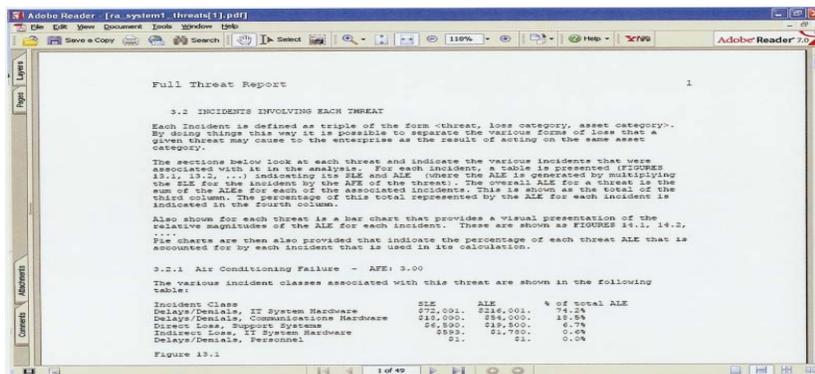
Full Asset Report

(Not Working at this time.)

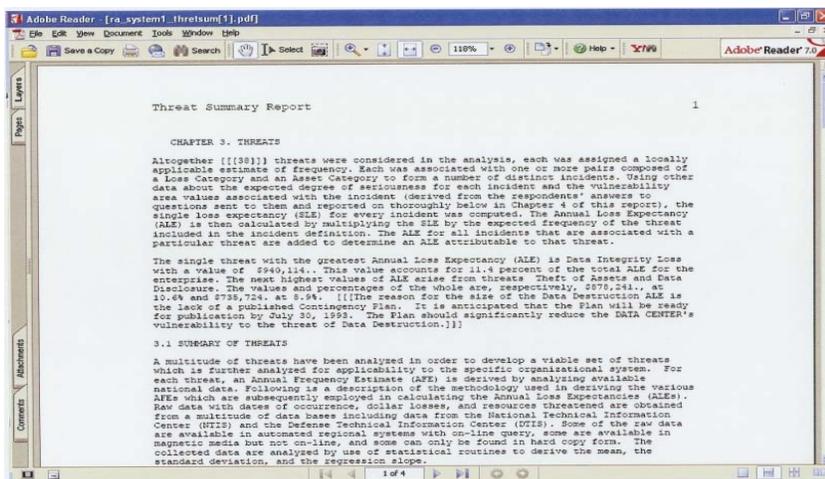
Summary By Asset Report



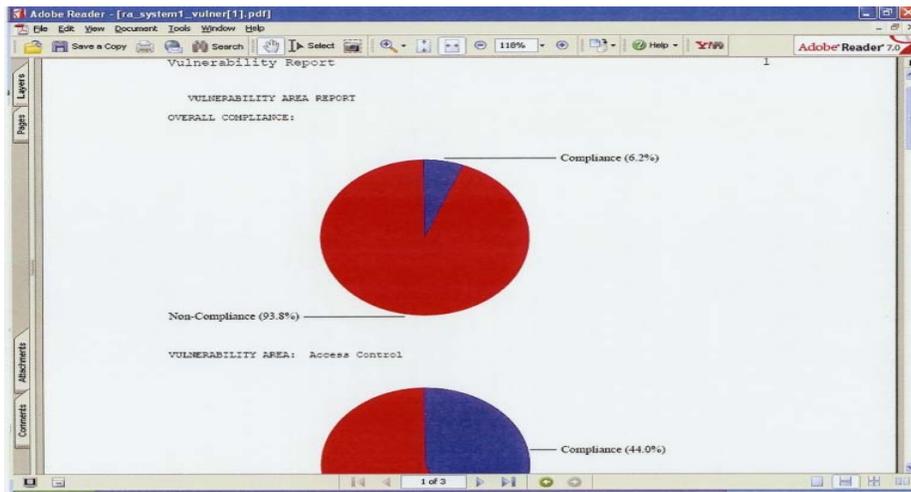
Full Threat Report



Summary By Threat Report



Full Vulnerability Report



Full Safeguard Report

Safeguard Report

5.2 FULL SAFEGUARD REPORT

This report contains information about each safeguard evaluated, based on the results of a full Cost-Benefit Analysis. This analysis used the reduction in ALE (cost savings), expected annually, and the safeguard costs over the lifetime of the safeguard to calculate the net present values provided in the following paragraphs at annual discount rates of 5%, 10%, and 15%.

5.2.1 Physical Access Control

Lifetime: 3 Implementation Cost: \$2,000,000. Annual Maintenance Cost: \$500,000.

Year	Benefits	Costs	Disc. Ben(0.1)	Disc. Cost(0.1)	DB-DC(0.1)
1	\$1,709,459.	\$2,000,000.	\$1,554,953.	\$1,818,181.	\$-264,126.
2	\$1,709,459.	\$500,000.	\$1,412,776.	\$413,223.	\$999,553.
3	\$1,709,459.	\$500,000.	\$1,284,341.	\$375,657.	\$908,684.

Sum of discounted benefits (0.05): \$4,659,280.
Sum of discounted benefits (0.1): \$4,251,170.
Sum of discounted benefits (0.15): \$3,903,079.
Sum of discounted costs (0.05): \$2,750,193.
Sum of discounted costs (0.1): \$2,607,061.
Sum of discounted costs (0.15): \$2,445,959.
Benefit Cost Ratio (0.05): 1.67
Benefit Cost Ratio (0.1): 1.63

Cost Benefit Report

Cost Benefit Report

CHAPTER 5. SAFEGUARDS

Based on the results of our risk analyses, a total of [16] safeguards are recommended for implementation to correct the deficiencies identified. The Safeguard Evaluation analyzed the identified safeguards determining the cost savings (Benefits) associated with each safeguard and the reduction in ALE derived if the safeguards were employed, and then used these values along with the safeguard costs to rank the safeguards in priority order based on return on investment (ROI).

It is generally accepted that safeguards can fall into three categories:

- (1) those that prevent incidents;
- (2) those that permit the timely detection of incidents that have not been detected;
- (3) those that aid in the recovery process after an incident has occurred.

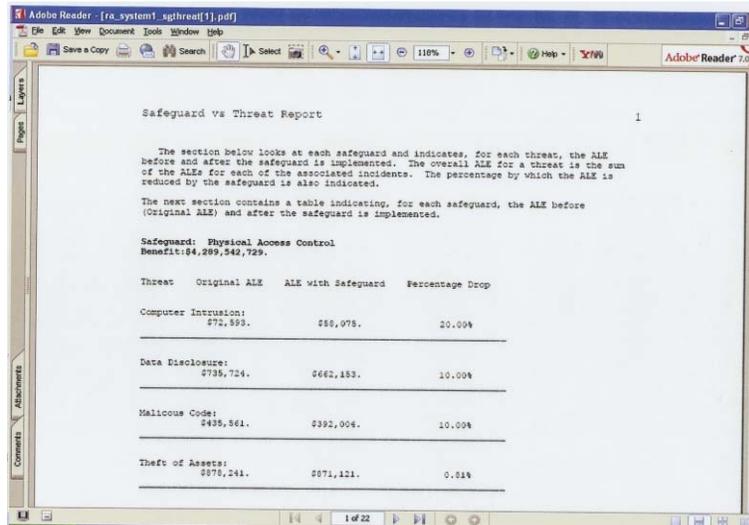
The goal of a safeguard is to reduce the Annual Loss Expectancy (ALE) of one or more risk events (incidents), thereby reducing the overall ALE for the enterprise. This reduction was calculated by considering how various safeguards impact the overall ALE in two different ways:

- (1) the reduction in the level of vulnerability in certain areas, and
- (2) the reduction in the frequency of a threat (or threat event).

5.1 COST-BENEFIT ANALYSIS

Not only is a safeguard intended to reduce ALE; it must also do it in a cost-effective way. A full Cost-Benefit Analysis was performed, which considered all identified safeguards and their impact on the overall ALE. This analysis used the reduction in ALE (cost savings), expected annually, and the safeguard costs over the lifetime of the safeguard to calculate the net present values provided in the tables below at annual discount rates of 5%, 10%, and 15%.

Safeguard Threat Report



Safeguard vs Threat Report

The section below looks at each safeguard and indicates, for each threat, the ALE before and after the safeguard is implemented. The overall ALE for a threat is the sum of the ALEs for each of the associated incidents. The percentage by which the ALE is reduced by the safeguard is also indicated.

The next section contains a table indicating, for each safeguard, the ALE before (Original ALE) and after the safeguard is implemented.

Safeguard: Physical Access Control
Benefit: \$4,299,542,729.

Threat	Original ALE	ALE with Safeguard	Percentage Drop
Computer Intrusion:	\$72,593.	\$58,075.	20.00%
Data Disclosure:	\$735,724.	\$662,153.	10.00%
Malicious Code:	\$425,561.	\$382,004.	10.00%
Theft of Assets:	\$370,241.	\$371,121.	0.01%

Note: Remember to close the report page to return to the Risk Assessment page. OCS has determined that only the Case Summary Report is needed for the C&A package. But all the reports need to be available if questions arise.

Appendix A

Things to do before starting a risk assessment:

- 1) Form a risk assessment team
- 2) Identify respondents from each functional area
- 3) Figure out your asset inventory using figures and tables in Appendix B. See Appendix C for example asset inventory.
- 4) List your safeguards and % implemented – include cost to implement and annual maintenance. See Appendix D for a glossary of safeguard terms.
- 5) The Annual Loss Expectancy table is built in – you should review this list and make appropriate changes for your area. For further information visit the FEMA website and look at specific data for your region.
<http://www.fema.gov/about/regions/index.shtm>

Generate your reports and customize them for your site and systems.

1. **Executive Summary** – High level summary of the risk assessment, will give your Director a good summary. This may be the only report your facility Director may need, but make sure you have the following reports available to support the results.
2. **Full Threat Report** - Each Incident is defined as triple of the form <threat, loss category, asset category>. By doing things this way it is possible to separate the various forms of loss that a given threat may cause to the enterprise as the result of acting on the same asset category.
3. **Full Vulnerability Report** – Provides pie charts that depict compliance/noncompliance all vulnerabilities. If a particular category or area, such as Terminal Site, is rate at 100% compliance a pie chart will not be displayed. Also, sometime the program will show “There is no information available for this area of vulnerability”. This should not be a problem at this time
4. **Cost Benefit Report** - The Safeguard Evaluation analyzed the identified safeguards determining the cost savings (Benefits) associated with each safeguard and the reduction in ALE derived if the safeguards were employed, and then used these values along with the safeguard costs to rank the safeguards in priority order based on return on investment (ROI.).
5. **Safeguard – Threat Report** - The section below looks at each safeguard and indicates, for each threat, the ALE before and after the safeguard is implemented. The overall ALE for a threat is the sum of the ALEs for each of the associated incidents. The percentage by which the ALE is reduced by the safeguard is also indicated.

Appendix B

Risk Assessment Asset List

Asset List		# of units	Total
LAN Servers	\$7,500.00		
Work Stations	\$2,500.00		
Switches	\$15,000.00		
Thin Clients	\$800.00		
Laptops	\$1,500.00		
VistA Servers	\$175,000.00		
Routers	\$85,000.00		
PBX Switches			
Video Surveillance System			
Wireless Hub System			
Card Access System			

Example Of Asset Costs for 3000 Employees

Asset Category	Asset Name	Specific Asset Description (number of devices)	Replacement Cost for the asset.	Cost per hour of unavailability of the asset measured to include.	A constant detection cost (or Auditing cost) for this asset.	Total Potential Cost to the Enterprise arising from this asset.	Percentage of mission dependent on this asset.
IT System Hardware	Windows Servers	23	\$172,500	\$15,000.00	\$17,250.00	\$204,750.00	20%
IT System Hardware	Work Stations	1700	\$4,250,000	\$18,750.00	\$425,000.00	\$4,693,750.00	25%
IT System Hardware	Switches	20	\$300,000	\$15,000.00	\$30,000.00	\$345,000.00	20%
IT System Hardware	Routers	20	\$1,700,000	\$15,000.00	\$170,000.00	\$1,885,000.00	20%
IT System Hardware	Thin Clients	700	\$560,000	\$22,500.00	\$56,000.00	\$638,500.00	30%
IT System Hardware	Laptops	125	\$187,500	\$2,250.00	\$18,750.00	\$208,500.00	3%
IT System Hardware	Vista Servers	3	\$255,000	\$37,500.00	\$18,750.00	\$243,750.00	50%
IT System Hardware	PBX	3	\$255,000	\$30,000.00	\$25,500.00	\$310,500.00	40%
IT System Hardware	Video Surveillance	3	\$255,000	\$7,500.00	\$25,500.00	\$288,000.00	10%
IT System Hardware	Wireless Hubs	3	\$255,000	\$15,000.00	\$25,500.00	\$295,500.00	20%
IT System Hardware	Card Access System	3	\$255,000	\$2,250.00	\$25,500.00	\$282,750.00	3%

An Interactive Excel Spreadsheet for you to fill in your information is provided by clicking the link below:

[**IT Risk Assessment Hardware Calculation Tool**](#)

Appendix C

Glossary of Safeguards

APPLICATION CONTROLS - The Application Controls safeguard refers to system controls designed by internal auditors/security staff to ensure universal programming standards, data element dictionaries, and record association conventions are maintained.

AUDIT TRAILS - The safeguard of Audit Trails refers to having a fully implemented audit trail capability, which identifies and tracks each system user and logs each transaction performed (transaction type, date, time, etc.).

CLASSIFICATION MARKINGS - The Classification Marking safeguard refers to having the data classification marked on the top and bottom of each page of all media and reports that contain sensitive, proprietary, and Privacy Act data.

CONTINGENCY PLAN - This safeguard refers to having a Contingency Plan (may be a Continuity of Operations Plan or Disaster Recovery Plan) containing detailed backup procedures to be followed in case of emergency disruption to network/computer resources.

CONTRACT SPECIFICATIONS - This safeguard refers to the practice of requiring each contractor to include as a formal contract deliverable, a plan for including appropriate security controls addressing pertinent vulnerabilities and threats.

DATA ENCRYPTION - The Data Encryption safeguard involves the application of encryption techniques to one or more datasets and to data transmitted over network and communications systems.

DETECTION SYSTEMS - This safeguard refers to having coordinated fire detection and access violation detection systems that will alert authorities to smoke, heat, water, humidity changes, grounding problems, as well as to access control violations.

DOCUMENTATION - The Documentation safeguard refers to the organization having backup documentation for every system, file, program, and process including hard copies retained in a safe location.

ELECTRICAL POWER - The Electrical Power safeguard refers to the establishment of a stable source of electrical power, including consideration of uninterruptible power sources and backup generators.

EMERGENCY RESPONSE - The Emergency Response safeguard refers to having a detailed plan and procedures to ensure the organization can continue to operate in the event of large scale emergencies (chemical spills, aircraft accidents, nuclear mishaps, etc.).

FILE/PROGRAM CONTROL - The safeguard of File/Program Control refers to the practice of establishing a system of data access controls (DACs) and authorizations for programs and files based on the "principle of least privilege".

FIRE SUPPRESSION - The Fire Suppression safeguard refers to the appropriate combination of water and CO2 that should be installed in any facility, including network operations facilities and data centers.

GROUNDING SYSTEMS - The safeguard of Grounding Systems refers to implementing proper electrical grounding systems for all equipment, including lightning arrestors and a separate grounding system for all signal cables.

LIFE CYCLE MANAGEMENT (LCM) - This safeguard refers to having a formal LCM plan for each system that defines the system LCM program, including system design, implementation, maintenance, funding, oversight, and security requirements.

MATERIAL SEGREGATION - The Material Segregation safeguard refers to the practice of separating classified, sensitive, proprietary, trade secret, and Privacy Act data from all other material to guard against inadvertent disclosure.

MONITORING/INTRUSION DETECTION SYSTEM - Refers to having an effective system in place to monitor and detect unauthorized intrusions into critical system components, operational application programs, sensitive files/databases, and remote computer systems.

NEW CONSTRUCTION - The New Construction safeguard covers a variety of protections that should be considered for any existing or new facility. For example, the use of fire retardant and low combustion building materials.

OPERATING PROCEDURES - This safeguard refers to having a monitoring program in place to determine the effectiveness and efficiency of the system's operating procedures, including monitoring to ensure these procedures are properly followed.

OPR FOR EACH SYSTEM - This safeguard refers to designating an Office of Primary Responsibility (OPR) for each database, data file, and removable media containing sensitive data or programs. The OPR designation is required to ensure data integrity.

ORGANIZATIONAL STRUCTURE - Organizational Structure refers to the safeguard of having the organization not only adequately staffed, but also responsive to the need for redundancy of critical job functions.

PASSWORDS/AUTHENTICATION - The safeguard of Passwords/Authentication refers to the organization having effective policy and procedures for protecting user passwords and other authentication controls, which are fully implemented for every system.

PERSONNEL CLEARANCES - The safeguard of Personnel Clearances refers to having policy and procedures to ensure that each system user has an equal or greater clearance than the highest classification level of data processed by or stored on the system.

PERSONNEL CONTROL - This safeguard refers to having procedures for conducting background checks before granting system access based on "need to know" and for updating access control and personnel records when people transfer or terminate employment.

PHYSICAL ACCESS CONTROL - The Physical Access Control safeguard refers to the existence of a verifiable, coordinated access control system. The system can range from simple (key lock systems) to complex (cipher locks/key card identification systems).

PREVENTIVE MAINTENANCE - The Preventive Maintenance safeguard refers to having an effective maintenance program for all systems and equipment, including computer hardware, generators, HVAC equipment, and fire systems.

PROPERTY MANAGEMENT - The Property Management safeguard refers to the organization having a comprehensive and effective program for property inventory control, allocation, and accountability.

QUALITY ASSURANCE - The Quality Assurance safeguard refers to establishing a program for regularly monitoring (and finding ways to improve) programming quality, user error rates, security controls effectiveness, computer systems responsiveness, etc.

REDUNDANT POWER - The safeguard of Redundant Power refers to having a secondary independent source of electrical power to backup the primary power source.

REVIEW SENSITIVE APPLICATIONS - The Review Sensitive Applications safeguard refers to the organization conducting a formal risk assessment of each sensitive application program on a regular basis.

RISK ASSESSMENT - The Risk Assessment safeguard refers to having recently conducted a formal risk assessment of each major system and application program and to having a policy requiring at least annual follow-up risk assessments.

SECURITY CLASSIFICATION - This safeguard requires the implementation of policy and procedures to ensure the proper classification of sensitive data and materials, including a receipt program and general handling procedures for all sensitive data.

SECURITY PLAN - The Security Plan safeguard refers to a formal, written plan that defines the responsibilities and tasks of the security staff and documents the security procedures necessary for protecting organizational assets.

SECURITY POLICY - The Security Policy refers to a formal, written policy that defines the guidelines that dictate how the organization manages its resources and protects them from both internal and external threats.

SECURITY STAFF - The Security Staff safeguard refers to the individuals in the organization who manage and perform security tasks full-time, as well as other

managers who have part-time security responsibilities for the resources they manage.

SYSTEM VALIDATION - The System Validation safeguard refers to the practice of ensuring that the operating system contains only approved code and that changes to the operating system are accounted for, verified, and transmitted securely.

TECHNICAL SURVEILLANCE - This safeguard refers to a team of security professionals (possibly from an external organization) who can conduct system technical vulnerability and penetration testing to identify system security problems.

TOTAL POTENTIAL COST TO ORGANIZATION - If Asset Is Contaminated, Damaged, Destroyed, or Disclosed Improperly (The total cost for illegal disclosure of Privacy data would potentially include legal fees, victim monetary awards, and Federal fines.)

TRAINING - The Training safeguard refers to the organization having implemented a formal and effective security training program for new employees, as well as recurring security awareness training programs for current employees.

VISITOR CONTROL - The Visitor Control safeguard refers to ensuring that visitors to a facility are monitored twenty-four hours a day, that a visitor audit trail exists, and that this official record is maintained for at least two years.

WATER DRAINAGE - This safeguard refers to facilities being equipped with adequate water drainage systems to ensure that water from broken pipes, water from activated sprinkler systems, or water used in fire fighting can be easily and effectively drained.