Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Defining a Risk Assessment Process for Federal Security Personnel

One goal of this paper is to provide general guidance on security resources for federal information system security officers within a federal agency. Another goal is to provide a basic template or outline for preparing to conduct a risk assessment as part of the agency's electronic and physical systems accreditation and certification process as required by Office of Management and Budget (OMB) Circular No A-130, Appendix III, the Computer Act of 1987, and other federal mandates.

Copyright SANS Institute
Author Retains Full Rights

AD

Kathleen Federico Version 1.3 December 2001

Please note that some hyperlinks work just fine if typed in at the browser but occasionally will not link correctly when accessed from this paper, in particular the FIPS links.

Defining a Risk Assessment Process for Federal Security Personnel

Overview

One goal of this paper is to provide general guidance on security resources for federal information system security officers within a federal agency. Another goal is to provide a basic template or outline for preparing to conduct a risk assessment as part of the agency's electronic and physical systems accreditation and certification process as required by Office of Management and Budget (OMB) Circular No A-130, Appendix III, the Computer Act of 1987, and other federal mandates.

Quick Review of Security

In order to cover this aspect of security appropriately, a brief overview of security and its goals is in order before delving into risk assessment. Security is not a new concept. People have been protecting their assets since the beginning of time. The moat around the castle, the deterents around some revered momento, locks on doors, rocks against a cave intrance – all processes put in place to deter or slow the potential thief or intruder. A universal definition of security involves protecting automated information systems in order to achieve the objectives of preserving the *confidentiality*, *integrity* and *availability* of all information system resources including software, data, and hardware.

Confidentiality – protecting the information resources from disclosure to unauthorized individuals.

Integrity – maintaining the accuracy, timeliness, consistency and completeness of information resources with a focus on data and system integrity. Data integrity is assuring that data is changed only as authorized by appropriate mechanisms. System integrity is a system running unimpaired from unauthorized changes or manipulations either intended or accidental.

Availability – Information systems and services are running at all specified times.

Securing one's systems and physical assets is a never-ending cycle as new technologies and threats arrive on scene at increasing rates. Consider the multitude of threats that may plague one's systems and physical structures. These threats may come from within the agency or from outside the agency. Protecting one's systems then becomes a daunting task because of the constant changing of players including people, software and hardware. Because of this ever changing playing field, the threats and perceived risks also change. To keep up, system administrators and security personnel must continually receive training and conduct research on the current state of affairs with the software or hardware platforms in use at their agency. In turn, the training and research will lead to continued monitoring, modifications, and retesting of these modifications to assure the best possible practices and security measures are consistently

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

being applied to their policies, procedures and systems. Additionally, there are innumerable new and revised Federal guidelines and laws that need to be considered and implemented.

It is more important now than ever that Federal computer systems, networks, and buildings be adequately protected from all types of threats and vulnerabilities. The Federal Government has mandated government-wide security, accountability and mandatory reporting requirements to help assure the public that the government information architecture and physical structures are secured to the best possible level. According to Executive Order on Critical Infrastructure Protection, "The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communication systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission areas. Cost-effective security shall be built into and made an integral part of government information systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations."[1]

Internet Links to Useful Security Sites

Following are some links to some of the Federal mandates and agencies designed to assist Federal agencies in their quest for secure infrastructures that may help those delegated the responsibility of implementing security. The lists that follow are by no means all-inclusive.

http://www.sans.org/	SANS Institute: Publications including step by step guides, security newsbytes, SANS Reading Room, security certification information, other security links and much more
http://www.cert.org/	CERT Coordination Center: Internet security expertise, training, security alerts and solutions, reading rooms, advisories, computer incidence response and much more
http://www.nist.gov/	National Institute of Standards and Technology: Contains Federal Information Processing Standards (FIPS) Publications, NIST Special Publications, and much more
http://www.nsa.gov/	National Security Agency:

[1] Executive Order on Critical Infrastructure Protection, October 16, 2001 http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	Good source for Cryptology information, security guides, and more
http://irm.cit.nih.gov/policy/aissp.html	Automated Information Systems Security Program Handbook (AISSP)
http://www.fedcirc.gov/	Federal Computer Incidence Response Center: Wealth of computer security information including advisories, tools, reporting requirements for federal agencies on intrusions, viruses, etc., patches, publications and much more
http://www.nipc.gov/	National Infrastructure Protection Center: Issues warnings, investigates incidences, works with law enforcement, trains, published vulnerabilities, warnings, and other security related items
http://www.hhs.gov/read/irmpolicy/	Health & Human Services: IRM Policy for all areas of IT
http://www.firstgov.gov/us_gov/legislative_branch.html	Legislative Links
http://www.nsi.org/	National Security Institute: Security information Industry and product news, Security information and library, legislation, technology
http://www.nara.gov/fedreg/plawwhat.html	Public Laws
http://www.gao.gov/special.pubs/cit.html	Government Accounting Office (GAO): Special Publications on Computer Information Technology
http://www.securityfocus.com/	BugTraq Tool for security professionals to track advisories, vulnerabilities, email notices
http://www.symantec.com/	Norton Antivirus/Firewall, etc.
http://www.microsoft.com/technet/default.asp	Microsoft TechNet and Microsoft Security Links
http://www.mcafee.com	McAfee Antivirus, etc.
http://www.iss.net	Internet Security Systems - For recently discovered vulner-abilities

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://www.mitre.org/	Common vulnerabilities and exposures and other security information
Own Agency's Security Web Pages	Example: HHS
Own Agency's Maintenance and Support Web Sites	Example: Cisco.com

Legislation or Federal Security Documents

The following list is not intended to be an exhaustive listing of legislation and special documentations addressing computer security in general. It is only provided as a starting point for one delving into the realm of Federal systems security. Each individual should also research and reference their own agencies specific policies and procedures for further definition of their particular requirements for securing their enterprise.

Executive Order on Critical Infrastructure Protection October 16, 2001	Order to ensure the protection of information systems for critical infrastructure, physical assets, and emergency preparedness communications
Executive Order Establishing Office of Homeland Security October 8, 2001	Establishes Office of Homeland Security and defines it responsibilities including Agency physical and information security
Computer Security Act of 1987 P.L. 100-235	Requires agencies to identify sensitive systems, conduct computer security awareness training, and develop computer security policies. Assigns National Institute of Standards and Technology (NIST) responsibility for developing standards and guidelines to assist agencies with implementing cost-effective security practices. NIST is to obtain assistance or advise from the National Security Agency (NSA)
44 U.S.C. Chapter 35	U.S. Code providing senior management officials with the responsibility for the security of federal information systems
Federal Information Resources Management Regulation (FIRMR)	Primary regulation for use, management, and acquisition of computer resources for the federal government
Office of Management and Budget (OMB) Circular A-130 Appendix III	Amended in Nov. 2000 incorporating the requirements of the Computer Security Act and outlining responsibilities for national security directive. Contains a minimum set of controls for Federal information security programs and assigns agency responsibilities
Government Performance Results Act	Established performance based goals for

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(GPRA) 1993	government agencies and addresses required reporting
Government Information Security Reform Act Public Law 106-398 (GISRA) 10/30/2000	Amends the Paper Reduction Act of 1995. Addresses program management. Creates a standard management framework and evaluation for both unclassified and classified security systems. Mandates annual assessments of systems by the agency and Office of the Inspector General (GAO). The Chief Information Officer (CIO) and GAO must provide a written report of the assessment to OMB
Information Technology Management Reform Act and The Federal Acquisition Reform Act (Clinger-Cohen)	Requires the heads of Federal agencies to link IT investments to agency accomplishments and establish a process to select, manage and control IT investments
The Health Insurance Portability & Accountability Act of 1996 (HIPAA)	Requires health insurance portability, reduces health care fraud and abuse, creates national standards for health information, and improves the security and privacy of shared medical information and imposes penalties for non-compliance
Privacy Act 1974	Outlines law covering records maintained on individuals and an agency's responsibilities pertaining to records
FIPS Publication 65	Guidelines for Automated Data Processing Risk Analysis
FIPS Publication 73	Guidelines for Security of Computer Applications
FIPS 102	Guidelines for Computer Security Certification and Accreditation
FIPS 87	Guidelines for ADP Contingency Planning
FIPS 31	Guidelines for ADP Physical Security and Risk Management
NIST Spec. Pub 800-18	Guide for Developing Security Plans for Information Technology Systems
NIST Spec. Pub 800-26	Security Self-Assessment Guide for Information Technology Systems
NIST Spec. Pub 800-27	Engineering Principles for Information Technology Security
NIST Spec. Pub 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
NIST Spec. Pub 800-21	Guideline for Implementing Cryptography in the Federal Government
NIST Spec. Pub 800-16	Information Technology Security Training

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	Requirements A Role and Performance Based Model
NIST Spec. Pub 800-12	An Introduction to Computer Security: The NIST Handbook
NIST Spec. Pub 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
NIST Spec. Pub 800-14	Generally Accepted Principles and Practices for Securing Information Systems
NIST Spec. Pub 800-10	Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls
NIST Spec. Pub 800-9	Good Security Practices for Electronic Commerce including Electronic Data Interchange
NIST Spec. Pub 800-4	Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials
NIST Spec. Pub 800-3	Establishing a Computer Security Incident Response Capability (CSIRC)
NIST Spec. Pub 800-5	A Guide to the Selection of Anti-Virus Tools and Techniques
NIST Spec. Pub 800/500 Series	Various areas of computer security including data encryption, passwords, secure telecommuting, VPNS and Firewalls, and many more topics
OCTAVE Catalog of Practices, Version 2.0 October 2001	Publication from CERT.org stands for Operationally Critical Threat, Asset and Vulnerability Evaluation Method the purpose of which is to assist agencies in identifying their critical assets and develop mitigation plans to address risks associated with these assets. It is a good guidance for those wishing to conduct self-directed risk evaluations
Agency Security Policies	Various policies available for each agency

Threats

A brief look at some of the threats to information systems resources and physical infrastructure would be helpful especially to the newcomer to security. This list is by no means inclusive and the definitions brief only intending to provide a glimpse into the threat. The reader interested in further exploring any of these areas and others not mentioned should refer to the references noted at the end of the paper or conduct further research of their own.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Social Engineering Techniques – An attacker technique used to exploit basic human instinct and gain unauthorized access to systems, physical plants or information. Example: Would be attacker calls the local IT support indicating that he is a systems developer working on an application problem but to verify it is fixed, he needs "root" access to the user's system. The support person gladly provides access.
- Hijacking a modem bypassing all firewall protection. Modems may be set to auto answer thus intruder may use tools, such as wardialers, readily available on the Internet to search for phone lines. Toneloc is one such wardialer. Modems at the desktop often do not require any authentication and can be accessed by anyone in a building and used for unauthorized access. Modem connections from a desktop using an Internet Service Provider are wide-open two directional connections that by-pass the firewall and thus, are suspectible to all the free scanning or interception tools.
- Malicious codes in the form of viruses, worms, Trojans, etc. Most agencies have experienced the wrath and loss of productivity due to malicious code including Melissa, I Love You, Anna Kournikova and of late, NIMDA and Code Red.
- Unencrypted transmission of sensitive agency, financial or patient data to those within the agency or outside which may result in some legal ramifications for the agency or in embarrassment or loss of public trust.
- Unauthorized access to or use of resources including disk drive capacity, CPU time, applications, files or services.
- Session Hijacking requires a highly technical attacker but nonetheless does occur. The hacker intercepts one end of a TCP communication exchange even after the strong authentication phase occurs. The attacker "spoofs" or fakes the original IP address, takes over the transmission. The correct pattern of sequence and acknowledgement numbers are then sent and the original party is prevented from participating in the transmission without their knowledge. Launching a denial of service or sending a TCP connection-reset command to the original party can accomplish this.
- Denial of Service (DOS) Attacks. It is the intent of a DOS to cripple the single target with service or activity requests so it can no longer service the requests of legitimate users. This is one of the easiest attacks to accomplish and is one of the most common. Many are preventable by following documented instructions on sound security practices. Some examples are Smurf attacks, ping attack of death, WinNuke attacks, and Teardrop. Distrubuted Denial of Service (DDOS) attacks are more sophisticated and dangerous because they cripple large numbers of systems or an entire network at one time by secretly planting an agent software on many machines making them "zombies" which are controlled by a some type of master controller. The controller then directs the zombies to launch a coordinated simultaneous attack on the victim thus flooding the network with packets and disabling the victim.
- No backups or failure to test the integrity of existing backups. The threat is loss of data, corruption of data or unavailability of data.
- Domain Hijacking. There are no security mechanisms built into Domain Name Services (DNS). An attacker can take over the target DNS by using a DOS and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

then replace the target with its own DNS server and advertise it as the target. This results in falsification of information to unspecting users.

- Wireless computers and networks. This standard is not sufficiently secure though great effort is being exerted to improve its security. Packets may be snatched from the airwaves rather easily; a car outside the building with a wireless card can easily access a wireless network inside the building. There are several tools available on the Internet that can recover encryption keys, such as Airsnort and WebCrack.
- Natural Threats such as lightning, fire, floods. Potential loss of information or physical assets.
- Storage of sensitive records including financial data. The data may not be protected from unauthorized access and may be subject to theft, unauthorized manipulation, shredding or destruction.
- File Transfers. FTP servers may allow anonymous access and have a direct link back into the entire network. Users transfer important data in unencrypted form that gets intercepted. CD-Rom, diskette, and electronic transfer mechanisms may release sensitive files. Another example would be users obtain unauthorized access to sensitive files or directories. Downloading of unauthorized software, sexually explicit software or graphics, hacking or cleansing tools, or non-work related activities. There are many freely available tools on the Internet that allow file-sharing capabilities. GNUTELLA is one such tool, which acts as both a server and client to allow sharing of Internet files while searching other users files. Open shares have been exploited by such malicious code as Code Red.
- Power issues. The power goes out; perhaps the doors have no backup lock mechanism to maintain the security of the computer rooms or other sensitive areas of the building. Power goes out unexpectedly and the systems aren't protected resulting in either corruption or loss of date, thus compromised integrity; or, system is unavailble to users which may compromise the goal of the agency, such as patient care or loss of e-business.
- Building Access. No guard on duty so visitors to the building have access to all open areas. No log of access thus no log of accountability for incidences in the building. There may be no alarms to warn of intrusions or breakins.
- Server and desktop access. Ever walked by an open terminal? Many users do not have anti-virus or firewall software. Passwords are not often implemented for access to these systems or aren't changed regularly or are not strong enough to withstand a password cracker, which is readily available to anyone on the Internet.
- Email. Email may be easily "spoofed" or falsified. Employees may send sensitive data intentionally or unintentionally to an authorized user or the transmission may be intercepted. Email is not private and not secure. Many email clients or servers have not been correctly configured and routinely patched. Over the past few years many legal cases have been brought against government and business because of inappropriate use of email including slander, pornography, sexual harrassment, discriminatory content, and so on. Most everyone has experienced the aftermath of a malicious code attack – email being an excellent transport thus

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

causing downtime, lost productivity, frustration, lost revenue, potential loss of data and more.

- Operating System (OS) vulnerabilities. Microsoft and others regularly issue vulnerabilities and warnings. Incorrect system configuration or leaving the OS unpatched may provide an opening into one's network. Not reconfiguring, removing sample programs and removing default configurations may lead to exploits. One example, many installations of NT included Internet Information Server (IIS) but it often was never configured, patched or used. Code Red took advantage of this vulnerability to infect many systems.
- Disgruntled employee. May exploit an agency's system in an attempt to get back at the agency for some action bestowed on the employee or to prove a point to the agency.
- Hostile former employer. Sabotage conducted by using "insider information or knowledge" to defeat or avoid existing security mechanisms. One means may be an old priviledge account that should have been removed.
- Contracting, telecommuting. There may be contractors who have not passed a security audit but have access to sensitive data. Users may be dialing into a system from an unprotected source. As the line blurs between the office computers and home computers, it is more likely users will be storing sensitive work information, passwords, financial information, etc., on a home PC or laptop that are tempting targets for attackers.

Because the threats are so prevalent and the environment in a constant state of flux, it is necessary and mandated by Federal policy, regulation and guidelines, such as The Government Information Security Reform Act, October 2001, and OMB Circular A-130 that appropriate assessments be conducted annually by federal agencies to attain minimum security requirements. According to the AISSP Handbook, periodic risk analyses are to be conducted by each facility no less than every five years. This handbook defines who in the agency has responsibility for developing and conducting the risk assessment and management program and ultimately implementing processes or procedures to mitigate any weaknesses identified. It also provides many guidelines on conducting all aspects of information systems security.

Risk analysis is a procedure used to estimate potential losses that may result from system vulnerabilities and to quantify the damage that may result if certain threats occur. The ultimate goal of risk analysis is to help select cost-effective safeguards that will reduce the risks to an acceptable level.[2] The evaluation should take into consideration all physical assets including the buildings, computers, and other equipment and, of course, the information contained therein. An assessment should look at the various types of information maintained by the agency to determine how important it is, how vulnerable it is, the cost of losing the information, and the cost of protecting it. One should keep in mind that though it is difficult to attach a cost to the loss of public image or loss of public confidence these two factors must play into the evaluation of any potential threat or loss. It is important also to remember that the cost of securing a system shouldn't exceed the financial and administrative cost of recovering the information or replacing the system unless it is in the interest of national defense or some other level of need.

[2] Russell, Deborah, and Gangemi, G.T., Sr., *Computer Security Basics*, p. 91, O'Reilly and Associates. 1991

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A risk assessment is designed to assess the security posture of a system or application from the manager's viewpoint with the purpose of raising the manager's awareness of the major security risks in their infrastructure and to propose recommendations for mitigation of these risks. One way to conduct such an assessment is via a facilitated risk assessment (FRA). There are many other methods of conducting risk assessments; this is not necessarily the best method or the worst method. A facilitator(s) and members of the agency's staff representing key aspects of the system or applications of the agency guide the assessment. The makeup of the group should include developers, program management, general users and approving authorities. They then work together to identify the assets of the agency, a common set of threats, vulnerabilities and countermeasures for the specific security architectural components of their respective systems. They will also define what the current state of security is for the system and develop suggested additional security requirements for the system being evaluated. Their ultimate goal is to produce a working document that will serve in managing resources and prioritizing security efforts for the agency.

The review may last several days and should allow all participants equal opportunity to contribute to the collective view of mission, funding, requirements, design, and operational procedures used to examine the risk associated with the system. A facilitator and recorder should be part of the process to keep things moving in an orderly fashion and to remove the task of documenting the process from the participants. Often it is advantageous to the agency to hire someone who is experienced in conducting such assessments for security and networks; and who can perform the preliminary research and preparation involved in conducting such an assessment. At the same time, it is critical to involve employees working in the program areas defined as critical as mentioned above. There is no better source of what the true picture of the program is and it's present security practices. Each role of the participants needs to be clearly defined at the start of the whole process and may include such roles as Designated Approving Authority, Facilitator, Program Management Office, User, Developer, and Recorder. Federal mandates and agency security policies and procedures need to be reviewed and compiled to develop a plan of action for the FRA team to work from to obtain the best results. A systems analysis to determine the boundaries of a system, the sensitivity and criticality of the information contained therein, processed by, or transmitted by the system and organizational responsibilities must be made at the outset of conducting a risk assessment and/or self-assessment. The facilitator prior to the start of the FRA could accomplish this by conducting interviews and gathering information from key folks within the agency. This information may be used to determine who will be the team members for the FRA. In addition, a security plan for all interconnected systems must be developed or may be accomplished as an outcome of the risk assessment. A risk assessment should be conducted prior to or in parallel with a self-assessment.

Possible Phases of an FRA Process

Phase One - Organizational Evaluation

The team determines the agency's most critical assets and identifies what is currently being done to secure these assets. During the information gathering stage the identity of the stakeholders may become evident. There should be representatives on the team from each program having a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

stake in the system. The trained facilitator will use many tools to elicit the information from the team members. Part of the preliminary preparation may include:

1) Interviewing senior management officials to determine their level of knowledge of critical assets, current security practices and perceived threats and organizational vulnerabilities.

2) Interviewing program managers to determine the same items as discussed with senior management.

3) Interviewing the IT staff assigned responsibilities for the assets identified by the first two groups of interviewees gathering the same information as the above.

4) The facilitator may then use this information to create threat profiles to use as a tool for assisting the FRA team in accomplishing its goals.

Phase Two - Identifying Infrastructure Vulnerabilities

The team will work together to analyze the components of the critical system to ascertain the weaknesses and potential for harm to these assets. Some of the processes may include:

1) Description of the System
    a. Discussion of the validity of the current Security Policy to determine if changes are necessary.
    b. Discussion of the concepts of operating the system to assess whether changes are needed.
    c. Discussions of all components of the system to assure all team members have a common understanding of the hardware, software and security features in use at the facility.
    d. Determine the stakeholders for each critical system.

2) Identification and Description of Potential Threats, Vulnerabilities and Countermeasures
    a. Defining the definition of a threat, vulnerability and countermeasure
        i. Threat – any person, activity, or event with the potential to cause harm to a system. Threats may be categorized as natural disaster, accidental, and intentional. The accidental and intentional may come from inside or outside the agency. Statistics show that insiders pose a greater threat because of their access to the agency's systems.
        ii. Vulnerability – an inherent weakness or flaw in the physical layout, system design, procedures, management, administration, personnel, hardware or software that may be exploited to cause harm to the system or physical plant.
        iii. Countermeasure – a technical or management control that detects or minimizes the impact of the threat or vulnerability.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

b. Identifying and/or verifying the potential threats to the critical system being identified. This may involve using the threat profiles from the preliminary information-gathering phase.
c. Examining the critical system for technology weaknesses or vulnerabilities and defining these against the potential threats.

Phase Three - Develop a Security Strategy and Formulize Plans to Address Identified Risks

The team will identify the risks to its critical systems. They will further decide whether and how to address these risks.

1) Risk Determination
   a. Conduct the risk analysis resulting in a risk profile for each critical asset. The team will identify the impact of each threat to the critical components of the system. They will define the risks, develop criteria to evaluate the risks if the facilitator hasn't provided it, and finally, evaluate the risk impact based on the criteria.
   b. Assigning weights to the threats and vulnerabilities may be accomplished as follows though there are other methods of doing so.
      i. Determine a "probability" rating, numeric value, which is the likelihood of occurrence after countermeasures have been applied for each threat. A suggested valued structure might be from 1 to 5 with 5 being Very High and 1 being Very Low likelihood of occurrence after countermeasures have been applied.
         1. Example

Threat Description	Possible Countermeasure	Rating
Accidental Disclosure – The unauthorized or accidental release of medical, personal or otherwise sensitive information	Findings: Those with access to sensitive data may not be aware of need to protect it from unauthorized disclosure Countermeasures: Training, Warning Banners	Medium

      ii. Determine a "level of impact" or damage rating for the vulnerabilities, using a numeric value that represents the severity of the impact after the countermeasures have been applied to the vulnerability. The same numeric scale used for threats could be applied where 5 represents Very High level of damage to 1 being No Measurable damage.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2) Determination of Risk
    i. Multiply the two values of probability and level of impact to determine a level of risk. This value will represent a relationship in which a specified threat attack might successfully exploit a specific vulnerability.

3) Discussion of Results of a. and b. above to make necessary adjustments to numeric value based on consensus from the team members resulting in a chart of high to low risks.

4) Identify Risk Mitigation Measures or Protection Strategy – High Risks Only
    a. FRA team identifies possible mitigation measures or countermeasures, discusses and votes on the measure based on its ability to effectively reduce the threat and/or vulnerability, the cost, and any possible schedule barriers.
    b. From knowledge gained during the FRA process, the team members discuss and make recommendations for the implementation of the mitigating strategies identified in the steps above, operational constraints of the system, allocation of any residual risk, and any future development or enhancements to the system. This may result in a table of threats, vulnerabilities, and countermeasures based on priority.
        i. Example

Priority	Countermeasure	Threats Addressed	Vulnerabilities Addressed
1	Establish training program for security personnel and system administrators	1,6,11	2,5

5) Results Documentation and Final Consensus of Team Members
    a. The recorder should continually document all ideas as they are presented or accepted and should verify the accuracy of it with the participants.
    b. Final Report should include the following:
        i. Executive Summary- short, concise and in lay terms defining briefly the reason for the report, who participated, the approach taken for the assessment, listing the most significant threats and vulnerabilities, define recommendations of the team by priority and cost factors if these were determined in the assessment. The above table may be a useful tool for presenting the results to management.
        ii. Table of Contents – may include the following:
            4. Sections
            5. Appendices
            6. List of Figures
            7. List of Tables
        iii. Introduction
            4. Purpose

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5. Scope
6. Background Information
7. Roles and Responsibilities of Team
8. List of References

iv. System Description

v. Approach of the Team

4. Overview of the Assessment Process
5. Architectural Analysis
6. Purpose of Team Participation
7. Verification and Testing of the Security Controls as Defined by the Team

vi. Detail of the Threats, Vulnerabilities, Countermeasures and Identified in the Review

vii. Conclusions and Recommendations by Priority

viii. Applicable Appendices (Should include a glossary of terms used in the report, checklists used, evaluation criteria, supporting research or documentation gathered and used to conduct the assessment, bibliography of references used, team members listing and titles, etc.)

c. Preparation of the final report is completed and provided to each participant for comments or recommended changes.

d. Changes are made after all members have responded back to the recorder or facilitator.

6) Presentation of Final Report to Management By Personnel Determined by the Agency or Team

7) Management Reviews, Refines, and Approves the Strategy and Plans

8) Testing and Implementation of the Strategies Outlined in the Final Risk Assessment Report

Now that the assessment is completed and management has given its seal of approval, attention can be focused on the following:

1) Adjust existing security policies to address results of the assessment
2) Develop additional policies/procedures if needed
3) Provide adequate training to security personnel and systems administrators
4) Continue to review, refine and test the effectiveness of security policies and procedures implemented at the agency
5) Continue to monitor and adjust systems, policies and procedures as indicated by the current world environment or in reaction to new threats, laws, etc.
6) Perform assessments of systems as required by federal mandates or earlier if there are indications that a significant change has occurred to a system.

There are many very detailed publications available to federal security personnel and systems administrators to assist them with not only conducting a risk assessment but also performing all

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

types of systems analysis for security processes. For example, the next table, taken from Indian Health Service literature[3], provides a quick glance at some of the minimum-security requirements mandated by the OMB Circulars, HIPAA, GISRA and JCAHO (Joint Commission for the Accreditation of Health Care Organizations). The table shows the requirement and then indicates which of the four regulations addresses that particular responsibility. One can quickly see that there is much overlap between the various regulations and the responsibilities imposed by each. It is hoped that this "cheat sheet" will save some time and effort for the individuals assigned to meet minimum security requirements and show that the task may not be as overwhelming as first imagined.

Automated Information Systems Security Program
Requirements and Source References

Minimum Security Requirements	GISRA	OMB Circulars	HIPAA	JCAHO
Program Responsibilities				
Implement and maintain AISSIP: assign responsibilities	X	X	X	X
Security Plans				
Identify sensitive systems, facilities and networks; implement security plans	X		X	X
Identify critical infrastructure assets; assess vulnerabilities	X			
Applications Security				
Certify systems; re-certify every 3 years	X	X	X	
Develop and maintain contingency plans and response procedures	X	X	X	X
Installation Security				
Conduct risk analysis every 3-5 years	X	X	X	
Prepare acquisitions specifications		X		
Maintain disaster recovery plans	X	X	X	X
Personnel Security				
Designate sensitive positions; screen incumbents	X		X	
Security Awareness Training				
Implement security awareness training	X	X	X	X
Reporting				
Report security weakness		X		
Develop security breach reporting system	X		X	

[3] Indian Health Service (IHS), *IHS Automated Information Systems Security Program Requirements and Source References*, 2002.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Develop incidence response capability	X		X	X
Establish security audit controls			X	
Physical Security				
Assign security responsibility and establish controls	X		x	
Protect access to work stations	X		X	X
Implement controls to protect against environmental hazards	X		X	
Protect access to computer rooms/data centers, server rooms, data closets	X		X	X

Conclusion

Federal agencies have many mandates to implement to 1) assure that systems and applications operate effectively and efficiently to meet the goals of confidentiality, integrity and availability; and 2) to minimize the level of risk and magnitude of harm that could result from loss, misuse, unauthorized access, or modification of information and 3) to provide adequate training to personnel assigned to implement the first two items. Without the proper training, implementation and attention to the security processes described in the myriad of federal regulations, policy, and law, no agency can be assured of an adequate level of security for their infrastructure. Performing risk and self-assessments to mitigate any weakness uncovered in the assessments is one way to determine if the agency has met its goal of acceptable security for its systems and the information contained therein. One will do well though to remember that there will never be a totally secure system, one can only strive to reduce the risk of attack, loss or damage to their systems to an acceptable level for their agency. Security requires the cooperation of all personnel within the agency to affectively implement a strong security initiative. This paper only provides a starting point for research for those assigned the challenging task of securing their agency's infrastructure.

References:

U.S. Department of Health and Human Services. *Automated Information Systems Security Program Handbook.*
URL: http://irm.cit.nih.gov/policy/aissp.html

General Accounting Office, *Information Security Risk Assessment Practices of Leading Organizations*, GAO Publication, November 1999
URL: http://www.gao.gov/special.pubs/ai00033.pdf

Office of Management and Budget (OPM). *Incorporating and Funding Security in Information Systems Investments.* Memorandum 00-07. February 28, 2000.
URL: http://www.whitehouse.gov/omb/memoranda/m00-07.html

National Institute of Standards and Technology (NIST). *Guide for Developing Security Plans for Information Technology Systems.* Special Publication 800-18. December 1998.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

URL: http://csrc.nist.gov/publications/nistbul/itl99-04.txt

U.S. Department of Commerce, NIST. Federal Information Processing Standards Publication (FIPS). *Guidelines for Security of Computer Applications. FIPS PUB 73. June 30, 1980.* URL: http://csrc.nist.gov/publications/fips/fips73/fips73.PDF

U.S. Department of Commerce, NIST. Federal Information Processing Standards Publication (FIPS). *Guidelines for Automatic Data Processing Physical Security and Risk Management.* FIPS PUB 31. June 1974.
URL: http://csrc.nist.gov/publications/fips/fips31/fips31.pdf

Microsoft. *Security Strategies.* URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bestprac/secstrat.asp

Alberts, Christopher J., Dorofee, Audrey J., and Allen, Julia H. *Octave Catalog of Practices*. Version 2.0. October 2001.
URL: http://www.cert.org/octave/methodintro.html

Office of Management and Budget. *Security of Federal Automated Information Resources.* OMB Circular A-130, Appendix III, Transmittal IV. November 28, 2000.

Guttman, Barbara and Roback, Edward A. *An Introduction to Computer Security: The NIST Handbook Computer Security*. Special Publication 800-12. NIST. October 1995.

Swanson, Marianne. *Security-Assessment Guide for Information Technology Systems Computer Security*. Special Publication 800-126. NIST. November 2001.

Pike, James. *Cisco Network Security.* Upper Saddle River, NJ. Prentice-Hall. 2002. Pg. 1-28.

Ardoin, Cy. Haynes, George. Nash, Barry. *Risk Assessment Reports for IHS.* 2001.

Indian Health Service *Automated Information Systems Security Program Requirements and Source References*. Developed by IHS Personnel. 2002.

Knudsen, Kent. *Risk Assessment in the University Setting.* SANS Reading Room. March 2001.

Rajasingham, Prabhacker. *Threat and Risk Assessments: Some Issues.* SANS Reading Room. April 2001.

Corrie, James. *Federal Systems Level Guidance for Securing Information Systems.* SANS Reading Room. August 2001.

Russell, Deborah and Gangemi, G.T., Sr. *Computer Security Basics.* Sebastopol, CA. O'Reilly & Associates. 1991. Pg. 89-10.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**