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.

An Introduction to Information System Risk Management

An understanding of risk and the application of risk assessment methodology is essential to being able to efficiently and effectively create a secure computing environment. Unfortunately, this is still a challenging area for information professionals due to the rate of change in technology, the relatively recent advent and explosive growth of the Internet, and perhaps the prevalence of the attitude (or reality) that assessing risk and identifying return on investment is simply too hard to do. This has kept information ...

Copyright SANS Institute
Author Retains Full Rights

AD

An Introduction to Information System Risk Management

© SANS Institute 2007, Author retains full rights.

Steve Elky

May 31, 2006

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1 Introduction....1
2 What Is Risk With Respect To Information Systems?....1
2.1 Threats....1
2.2 Vulnerabilities....2
3 Why Is It Important to Manage Risk?....3
4 How Is Risk Assessed?....3
4.1 Quantitative Risk Assessment....3
4.2 Qualitative Risk Assessment....4
4.2.1 Identifying Threats....5
4.2.2 Identifying Vulnerabilities....5
4.2.3 Relating Threats to Vulnerabilities....6
4.2.4 Defining Likelihood....6
4.2.5 Defining Impact....7
4.2.6 Assessing Risk....8
5 How Is Risk Managed?....9
5.1 Mitigation....9
5.2 Transference....9
5.3 Acceptance....9
5.4 Avoidance....9
5.5 Communicating Risks and Risk Management Strategies....10
5.6 Implementing Risk Management Strategies....10
6 What Are Some Common Risk Assessment/Management Methodologies and Tools?....11
6.1 National Institute of Standards & Technology (NIST) Methodology....11
6.2 OCTAVE®....12
6.3 FRAP....13
6.4 COBRA....13
6.5 Risk Watch....13
7 Summary....13

Table of Figures

Figure 1 – Partial List of Threats with Threat Sources Taken into Consideration....2
Figure 2 – Sample Likelihood Definitions....6
Figure 3 – Sample Impact Definitions....7
Figure 4 – Examples of Organizational Effect....8
Figure 5 – Sample Risk Determination Matrix....8
Figure 6 – Sample Risk Management Table....10
Figure 7 – Sample POAM....11

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1 Preface

This paper covers the basics of IT risk assessment. To learn more about this topic we recommend taking the SANS SEC410 IT Security Audit and Control Essentials course, available both online and via live classroom training.

2 Introduction

The fundamental precept of information security is to support the mission of the organization. All organizations are exposed to uncertainties, some of which impact the organization in a negative manner. In order to support the organization, IT security professionals must be able to help their organizations' management understand and manage these uncertainties.

Managing uncertainties is not an easy task. Limited resources and an ever-changing landscape of threats and vulnerabilities make completely mitigating all risks impossible. Therefore, IT security professionals must have a toolset to assist them in sharing a commonly understood view with IT and business managers concerning the potential impact of various IT security related threats to the mission. This toolset needs to be consistent, repeatable, cost-effective and reduce risks to a reasonable level.

Risk management is nothing new. There are many tools and techniques available for managing organizational risks. There are even a number of tools and techniques that focus on managing risks to information systems. This paper explores the issue of risk management with respect to information systems and seeks to answer the following questions:

- What is risk with respect to information systems?
- Why is it important to understand risk?
- How is risk assessed?
- How is risk managed?
- What are some common risk assessment/management methodologies and tools?

3 What Is Risk With Respect To Information Systems?

Risk is the potential harm that may arise from some current process or from some future event. Risk is present in every aspect of our lives and many different disciplines focus on risk as it applies to them. From the IT security perspective, risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. IT security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information.

Risk is a function of the ***likelihood*** of a given ***threat-source's*** exercising a particular potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization.[i]

3.1 Threats

One of the most widely used definitions of threat and threat-source can be found in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-30, Risk

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Management Guide for Information Technology Systems. NIST SP 800-30 provides the following definitions.

Threat: The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.[ii]

Threat-Source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.[iii]

The threat is merely the potential for the exercise of a particular vulnerability. Threats in themselves are not actions. Threats must be coupled with threat-sources to become dangerous. This is an important distinction when assessing and managing risks, since each threat-source may be associated with a different likelihood, which, as will be demonstrated, affects risk assessment and risk management. It is often expedient to incorporate threat sources into threats. The list below shows some (but not all) of the possible threats to information systems.

Figure 1 – Partial List of Threats with Threat Sources Taken into Consideration

Threat (Including Threat Source)	Description
Accidental Disclosure	The unauthorized or accidental release of classified, personal, or sensitive information.
Acts of Nature	All types of natural occurrences (e.g., earthquakes, hurricanes, tornadoes) that may damage or affect the system/application. Any of these potential threats could lead to a partial or total outage, thus affecting availability.
Alteration of Software	An intentional modification, insertion, deletion of operating system or application system programs, whether by an authorized user or not, which compromises the confidentiality, availability, or integrity of data, programs, system, or resources controlled by the system. This includes malicious code, such as logic bombs, Trojan horses, trapdoors, and viruses.
Bandwidth Usage	The accidental or intentional use of communications bandwidth for other then intended purposes.
Electrical Interference/ Disruption	An interference or fluctuation may occur as the result of a commercial power failure. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation).
Intentional Alteration of Data	An intentional modification, insertion, or deletion of data, whether by authorized user or not, which compromises confidentiality, availability, or integrity of the data produced, processed, controlled, or stored by data processing systems.
System Configuration Error (Accidental)	An accidental configuration error during the initial installation or upgrade of hardware, software, communication equipment or operational environment.
Telecommunication Malfunction/ Interruption	Any communications link, unit or component failure sufficient to cause interruptions in the data transfer via telecommunications between computer terminals, remote or distributed processors, and host computing facility.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

3.2 Vulnerabilities

Once again, NIST SP 800-30 provides an excellent definition of vulnerability as it pertains to information systems.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.[iv]

Notice that the vulnerability can be a flaw or weakness in any aspect of the system. Vulnerabilities are not merely flaws in the technical protections provided by the system. Significant vulnerabilities are often contained in the standard operating procedures that systems administrators perform, the process that the help desk uses to reset passwords or inadequate log review. Another area where vulnerabilities may be identified is at the policy level. For instance, a lack of a clearly defined security testing policy may be directly responsible for the lack of vulnerability scanning.

Here are a few examples of vulnerabilities related to contingency planning/ disaster recovery:

- Not having clearly defined contingency directives and procedures
- Lack of a clearly defined, tested contingency plan
- The absence of adequate formal contingency training
- Lack of information (data and operating system) backups
- Inadequate information system recovery procedures, for all processing areas (including networks)
- Not having alternate processing or storage sites
- Not having alternate communication services

4 Why Is It Important to Manage Risk?

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Therefore, risk management must be a management function rather than a technical function.

It is vital to manage risks to systems. Understanding risk, and in particular, understanding the specific risks to a system allow the system owner to protect the information system commensurate with its value to the organization. The fact is that all organizations have limited resources and risk can never be reduced to zero. So, understanding risk, especially the magnitude of the risk, allows organizations to prioritize scarce resources.

5 How Is Risk Assessed?

Risk is assessed by identifying threats and vulnerabilities, then determining the likelihood and impact for each risk. It's easy, right? Unfortunately, risk assessment is a complex undertaking, usually based on imperfect information. There are many methodologies aimed at allowing risk

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

assessment to be repeatable and give consistent results. Some of the leading methodologies are discussed in greater detail in Section 7.

The general process of risk assessment is discussed below.

5.1 Quantitative Risk Assessment

Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs.

Mathematically, quantitative risk can be expressed as Annualized Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realized over a one-year period.

ALE = SLE * ARO

Where:

- SLE (Single Loss Expectancy) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss.
- ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the likelihood.

Mathematically, this gets complicated very quickly, involving statistical techniques that are beyond the scope of this discussion.

While utilizing quantitative risk assessment seems straightforward and logical, there are issues with using this approach with information systems. While the cost of a system may be easy to define, the indirect costs, such as value of the information, lost production activity and the cost to recover is imperfectly known at best. Moreover, the other major element of risk, likelihood, is often even less perfectly known. For example, what is the likelihood that someone will use social engineering to gain access to a user account on the accounting system?

Therefore, a large margin of error is typically inherent in quantitative risk assessments for information systems. This might not always be the case in the future. As the body of statistical evidence becomes available, trends can be extrapolated on past experience. Insurance companies and financial institutions make excellent use of such statistics to ensure that their quantitative risk assessments are meaningful, repeatable and consistent.

Typically, it is not cost-effective to perform a quantitative risk assessment for an IT system, due to the relative difficulty of obtaining accurate and complete information. However, if the information is deemed reliable, a qualitative risk assessment is an extremely powerful tool to communicate risk to all level of management.

> Quantitative risk measurement is the standard way of measuring risk in many fields, such as insurance, but it is not commonly used to measure risk in

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

information systems. Two of the reasons claimed for this are 1) the difficulties in identifying and assigning a value to assets, and 2) the lack of statistical information that would make it possible to determine frequency. Thus, most of the risk assessment tools that are used today for information systems are measurements of qualitative risk.[v]

5.2 Qualitative Risk Assessment

Qualitative risk assessments assume that there is already a great degree of uncertainty in the likelihood and impact values and defines them, and thus risk, in somewhat subjective or qualitative terms. Similar to the issues in quantitative risk assessment, the great difficulty in qualitative risk assessment is defining the likelihood and impact values. Moreover, these values need to be defined in a manner that allows the same scales to be consistently used across multiple risk assessments.

The results of qualitative risk assessments are inherently more difficult to concisely communicate to management. Qualitative risk assessments typically give risk results of “High”, “Moderate” and “Low”. However, by providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization’s management.

5.2.1 Identifying Threats

As was alluded to in the section on threats, both threat-sources and threats must be identified. Threats should include the threat-source to ensure accurate assessment.

Some common threat-sources include:

- Natural Threats—floods, earthquakes, hurricanes
- Human Threats—threats caused by human beings, including both unintentional (inadvertent data entry) and deliberate actions (network based attacks, virus infection, unauthorized access)
- Environmental Threats—power failure, pollution, chemicals, water damage

Some common threats were illustrated in Figure 1 – Partial List of Threats with Threat Sources Taken into Consideration.

Individuals who understand the organization, industry or type of system (or better yet all three) are key in identifying threats. Once the general list of threats has been compiled, review it with those most knowledgeable about the system, organization or industry to gain a list of threats that applies to the system.

It is valuable to compile a list of threats that are present across the organization and use this list as the basis for all risk management activities. As a major consideration of risk management is to ensure consistency and repeatability, an organizational threat list is invaluable.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

5.2.2 Identifying Vulnerabilities

Vulnerabilities can be identified by numerous means. Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, start with commonly available vulnerability lists or control areas. Then, working with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system. Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives, such as Common Vulnerabilities and Exposures (CVE - http://cve.mitre.org) or the National Vulnerability Database (NVD - http://nvd.nist.gov). If they exist, previous risk assessments and audit reports are the best place to start.

Additionally, while the following tools and techniques are typically used to evaluate the effectiveness of controls, they can also be used to identify vulnerabilities:

- Vulnerability Scanners – Software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- Penetration Testing – An attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering
- Audit of Operational and Management Controls – A thorough review of operational and management controls by comparing the current documentation to best practices (such as ISO 17799) and by comparing actual practices against current documented processes.

It is invaluable to have a base list of vulnerabilities that are always considered during every risk assessment in the organization. This practice ensures at least a minimum level of consistency between risk assessments. Moreover, vulnerabilities discovered during past assessments of the system should be included in all future assessments. Doing this allows management to understand that past risk management activities have been effective.

5.2.3 Relating Threats to Vulnerabilities

One of the more difficult activities in the risk management process is to relate a threat to a vulnerability. Nonetheless, establishing these relationships is a mandatory activity, since risk is defined as the exercise of a threat against a vulnerability. This is often called threat-vulnerability (T-V) pairing. Once again, there are many techniques to perform this task.

Not every threat-action/threat can be exercised against every vulnerability. For instance, a threat of “flood” obviously applies to a vulnerability of “lack of contingency planning”, but not to a vulnerability of “failure to change default authenticators.”

While logically it seems that a standard set of T-V pairs would be widely available and used; there currently is not one readily available. This may be due to the fact that threats and especially vulnerabilities are constantly being discovered and that the T-V pairs would change fairly often.

Nonetheless, an organizational standard list of T-V pairs should be established and used as a baseline. Developing the T-V pair list is accomplished by reviewing the vulnerability list and

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

pairing a vulnerability with every threat that applies, then by reviewing the threat list and ensuring that all the vulnerabilities that that threat-action/threat can act against have been identified. For each system, the standard T-V pair list should then be tailored.

5.2.4 Defining Likelihood

Determining likelihood is fairly straightforward. It is the probability that a threat caused by a threat-source will occur against a vulnerability. In order to ensure that risk assessments are consistent, it is an excellent idea to utilize a standard definition of likelihood on all risk assessments.

Figure 2 – Sample Likelihood Definitions

	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

Be very careful in setting up the likelihood definitions. Figure 2 – Sample Likelihood Definitions shows a bell curve, with a Moderate being twice as significant as a Low or a High. This may be an unfair characterization for a particular organization that prefers to use a straight curve (Low: 0-33%, Moderate: 34-66%, High: 67-100%) or perhaps five levels of likelihood: Very Low, Low, Moderate, High and Very High. The most important thing is to make sure that the definitions are consistently used, clearly communicated, agreed upon and understood by the team performing the assessment and by organizational management.

5.2.5 Defining Impact

In order to ensure repeatability, impact is best defined in terms of impact upon availability, impact upon integrity and impact upon confidentiality. Figure 3 – Sample Impact Definitions illustrates a workable approach to evaluating impact by focusing attention on the three aspects of information security. However, in order to be meaningful, reusable and easily communicated, specific ratings should be produced for the entire organization. Figure 4 – Examples of Organizational Effect shows these specific values.

Figure 3 – Sample Impact Definitions

	Confidentiality	Integrity	Availability
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization.	Loss of availability leads to a **limited effect** on the organization.
Moderate	Loss of confidentiality leads to a **serious effect** on the organization.	Loss of integrity leads to a **serious effect** on the organization.	Loss of availability leads to a **serious effect** on the organization.
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Figure 4 – Examples of Organizational Effect

Effect Type	Effect on Mission Capability	Financial Loss/ Damage to Organizational Assets	Effect on Human Life
Limited Effect	Temporary loss of one or more minor mission capabilities	Under $5,000	Minor harm (e.g., cuts and scrapes)
Serious Effect	Long term loss of one or more minor or temporary loss of one or more primary mission capabilities	$5,000-$100,000	Significant harm, but not life threatening
Severe Effect	Long term loss of one or more primary mission capabilities	Over $100,000	Loss of life or life threatening injury

5.2.6 Assessing Risk

Assessing risk is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. When assessing likelihood and impact, take the current threat environment and controls into consideration. Likelihood and impact are assessed on the system as it is operating at the time of the assessment. Do not take any planned controls into consideration. Figure 5 – Sample Risk Determination Matrix can be used to evaluate the risk when using a three level rating system.

Figure 5 – Sample Risk Determination Matrix

		Impact		
		High	**Moderate**	**Low**
Likelihood	**High**	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

In a qualitative risk assessment, it is best not to use numbers when assessing risk. Managers, especially the senior level managers that make decisions concerning resource allocation, often assume more accuracy than is actually conveyed when reviewing a risk assessment report containing numerical values. Recall that in a qualitative risk assessment, the likelihood and impact values are based on the best available information, which is not typically well grounded in documented past occurrences.

The concept of not providing any more granularity in risk assessment reports than was available during the assessment process is roughly analogous to the use of significant digits in physics and chemistry. Roughly speaking, significant digits are the digits in a measurement that are reliable. Therefore, it is impossible to get any more accuracy from the result than was available from the source data. Following this logic, if likelihood and impact were evaluated on a Low, Moderate, High basis, Risk would also be Low, Moderate or High.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

If the risk assessment report does not clearly communicate the proper level of granularity, the number of impact and likelihood rating levels should be increased. Some organizations prefer to use a four or even five level rating for impact and likelihood. However, understand that the individual impact and likelihood levels must still be concisely defined.

6 How Is Risk Managed?

Recall that the purpose of assessing risk is to assist management in determining where to direct resources. There are four basic strategies for managing risk: mitigation, transference, acceptance and avoidance. Each will be discussed below.

For each risk in the risk assessment report, a risk management strategy must be devised that reduces the risk to an acceptable level for an acceptable cost. For each risk management strategy, the cost associated with the strategy and the basic steps for achieving the strategy (known as the Plan Of Action & Milestones or POAM) must also be determined.

6.1 Mitigation

Mitigation is the most commonly considered risk management strategy. Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw. A common mitigation for a technical security flaw is to install a patch provided by the vendor. Sometimes the process of determining mitigation strategies is called control analysis.

6.2 Transference

Transference is the process of allowing another party to accept the risk on your behalf. This is not widely done for IT systems, but everyone does it all the time in their personal lives. Car, health and life insurance are all ways to transfer risk. In these cases, risk is transferred from the individual to a pool of insurance holders, including the insurance company. Note that this does not decrease the likelihood or fix any flaws, but it does reduce the overall impact (primarily financial) on the organization.

6.3 Acceptance

Acceptance is the practice of simply allowing the system to operate with a known risk. Many low risks are simply accepted. Risks that have an extremely high cost to mitigate are also often accepted. Beware of high risks being accepted by management. Ensure that this strategy is in writing and accepted by the manager(s) making the decision. Often risks are accepted that should not have been accepted, and then when the penetration occurs, the IT security personnel are held responsible. Typically, business managers, not IT security personnel, are the ones authorized to accept risk on behalf of an organization.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

6.4 Avoidance

Avoidance is the practice of removing the vulnerable aspect of the system or even the system itself. For instance, during a risk assessment, a website was uncovered that let vendors view their invoices, using a vendor ID embedded in the HTML file name as the identification and no authentication or authorization per vendor. When notified about the web pages and the risk to the organization, management decided to remove the web pages and provide vendor invoices via another mechanism. In this case, the risk was avoided by removing the vulnerable web pages.

6.5 Communicating Risks and Risk Management Strategies

Risk must also be communicated. Once risk is understood, risks and risk management strategies must be clearly communicated to organizational management in terms easily understandable to organizational management. Managers are used to managing risk, they do it every day. So presenting risk in a way that they will understand is key. Ensure you do not try to use "fear, uncertainty and doubt." Instead, present risk in terms of likelihood and impact. The more concrete the terms are, the more likely organizational management will understand and accept the findings and recommendations.

With a quantitative risk assessment methodology, risk management decisions are typically based on comparing the costs of the risk against the costs of risk management strategy. A return on investment (ROI) analysis is a powerful tool to include in the risk assessment report. This is a tool commonly used in business to justify taking or not taking a certain action. Managers are very familiar with using ROI to make decisions.

With a qualitative risk assessment methodology, the task is somewhat more difficult. While the cost of the strategies is usually well known, the cost of not implementing the strategies is not, which is why a qualitative and not a quantitative risk assessment was performed. Including a management-friendly description of the impact and likelihood with each risk and risk management strategy is extremely effective. Another effective strategic is showing the residual risk that would be effective after the risk management strategy was enacted.

Figure 6 – Sample Risk Management Table

Risk	Risk Description	Impact	Likelihood	Risk Mgmt Strategy	Cost	Residual Risk After Implementing Risk Management Strategy
M[1]	Failure in environmental systems (e.g. air conditioning) leaves systems unavailable.	Failure in environmental controls could cause system to become unavailable for more than 48 hours.	Past data indicates this happens 1-2 times annually	Implement a hot spare at the alternate site	$250,000	L

[1] Moderate

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

6.6 Implementing Risk Management Strategies

A Plan Of Action & Milestones (POAM) should be part of the risk assessment report presented to management. The POAM is a tool to communicate to management on the proposed and actual completion of the implementation of the risk management strategies.

The first step in implementing risk management strategies is to get management to approve the POAM. Afterwards, the various individuals and teams report upon their progress. This in turn is reported to management and tracked as part of the ongoing process of risk management.

Figure 7 – Sample POAM illustrates a typical POAM. The POAM contains the risk, the risk management strategy, the Point Of Contact (POC) responsible for implementing the strategy, the resources required and the various milestones that comprise the implementation. For each milestone, a target completion date and an actual completion date is listed. Note that the POAM is a tool to communicate to management, rather than a project management plan.

Figure 7 – Sample POAM

Risk	Risk Mgmt Strategy	POC	Resources Required	Milestones	Target Completion Date	Actual Completion Date
Failure in environmental systems (e.g. air conditioning) leaves systems unavailable.	Implement a hot spare at the alternate site	Joe Smith	$100,000 hardware, $50,000 software, $100,000 labor	Procure hardware & software Install hardware Install software Configure system Test system	9/1 9/15 10/1 10/15 11/1	

7 What Are Some Common Risk Assessment/Management Methodologies and Tools?

There are numerous risk assessment/management methodologies and tools. The following methodologies and tools were developed for managing risks in information systems.

- National Institute of Standards & Technology (NIST) Methodology
- OCTAVE®
- FRAP
- COBRA
- Risk Watch

7.1 National Institute of Standards & Technology (NIST) Methodology

NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* is the US Federal Government's standard. This methodology is primarily designed to be qualitative and is based upon skilled security analysts working with system owners and technical experts to thoroughly identify, evaluate and manage risk in IT systems. The process is extremely

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

comprehensive, covering everything from threat-source identification to ongoing evaluation and assessment.

The NIST methodology consists of 9 steps:

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation

7.2 OCTAVE®

The Software Engineering Institute (SEI) at Carnegie Mellon University developed the Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE) process. The main goal in developing OCTAVE is to help organizations improve their ability to manage and protect themselves from information security risks. OCTAVE is workshop-based rather than tool based. This means that rather than including extensive security expertise in a tool, the participants in the risk assessment need to understand the risk and its components. The workshop-based approach espouses the principle that the organization will understand the risk better than a tool and that the decisions will be made by the organization rather than by a tool.

There are three phases of workshops. Phase 1 gathers knowledge about important assets, threats, and protection strategies from senior managers. Phase 1 consists of the following processes:

- Process 1: Identify Senior Management Knowledge
- Process 2: (multiple) Identify Operational Area Management Knowledge
- Process 3: (multiple) Identify Staff Knowledge
- Process 4: Create Threat Profiles

Phase 2 gathers knowledge from operational area managers. Phase 2 consists of the following processes:

- Process 5: Identify Key Components
- Process 6: Evaluate Selected Components

Phase 3 gathers knowledge from staff. Phase 3 consists of the following processes:

- Process 7: Conduct Risk Analysis
- Process 8: Develop Protection Strategy (workshop A: strategy development) (workshop B: strategy review, revision, approval)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

These activities produce a view of risk that takes the entire organization's viewpoints into account, while minimizing the time of the individual participants. The outputs of the OCTAVE process are:

- Protection Strategy
- Mitigation Plan
- Action List

7.3 FRAP

The Facilitated Risk Assessment Process (FRAP) is the creation of Thomas Peltier. It is based upon implementing risk management techniques in a highly cost-effective way. FRAP uses formal qualitative risk analysis methodologies using Vulnerability Analysis, Hazard Impact Analysis, Threat Analysis and Questionnaires. Moreover, FRAP stresses pre-screening systems and only performing formal risk assessments on systems when warranted. Lastly, FRAP ties risk to impact using the Business Impact Analysis as a basis for determining impact. Thomas Peltier has written a book on FRAP and several consulting companies, including RSA and Peltier Associates, teach FRAP.

7.4 COBRA

The Consultative, Objective and Bi-functional Risk Analysis (COBRA) process was originally created by C & A Systems Security Ltd. in 1991. It takes the approach that risk assessment is a business issue rather than a technical issue. It consists of tools that can be purchased and then utilized to perform self-assessments of risk, while drawing on the expert knowledge embedded in the tools. The primary knowledge bases are:

- IT Security (or default)
- Operational Risk
- 'Quick Risk' or 'high level risk'
- e-Security

There are two primary products, Risk Consultant and ISO Compliance. Risk Consultant is a tool with knowledge bases and built in templates that allow the user to create questionnaires to gather the information about the types of assets, vulnerabilities, threats, and controls. From this information, Risk Consultant can create reports and make recommendations, which can then be customized. ISO Compliance is similar, only this product is focused on ISO 17799 compliance.

7.5 Risk Watch

Risk Watch is another tool that uses an expert knowledge database to walk the user through a risk assessment and provide reports on compliance as well as advice on managing the risks. Risk Watch includes statistical information to support quantitative risk assessment, allowing the user to show ROI for various strategies. Risk Watch has several products, each focused along different compliance needs. There are products based on NIST Standards (U.S. government), ISO 17799, HIPAA and Financial Institution standards (Gramm Leach Bliley Act, California SB

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1386 (Identify Theft standards), Facilities Access Standards and the FFIEC Standards for Information Systems).

8 Summary

In summary, successful and effective risk management is the basis of successful and effective IT security. Due to the reality of limited resources and nearly unlimited threats, a reasonable decision must be made concerning the allocation of resources to protect systems. Risk management practices allow the organization to protect information and business process commensurate with their value. To ensure the maximum value of risk management, it must be consistent and repeatable, while focusing on measurable reductions in risk. Establishing and utilizing an effective, high quality risk management process and basing the information security activities of the organization on this process will lead to an effective information security program in the organization.

This paper covered some of the basics of IT risk assessment. To learn more about this topic we recommend taking the SANS SEC410 IT Security Audit and Control Essentials course, available both online and via live classroom training.

---

[i] National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 8

[ii] National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 12

[iii] National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 12

[iv] National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 15

[v] Horton, Thomas. "Managing Information Security Risks"

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced