Modelling, measuring and managing information technology risks

Stephen Elky
Deputy Director of Information Technology Services,
US Library of Congress, Washington, DC 20540

Abstract
An understanding of risk and the application of risk assessment methodology are 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 chapter explores risk modelling, measurement and management.

Keywords: Risk, Threat, Threat-source, Vulnerability, Qualitative Risk Assessment, Quantitative Risk Assessment, Likelihood, Impact, Risk Mitigation, Risk Transference, Risk Acceptance, Risk Avoidance, Threat Zone, Plan of Action & Milestones

1 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, information technology (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 level that is deemed reasonable by the organization, rather than the individual.

Risk management is nothing new. There are many tools and techniques available for managing organizational risks. There are a myriad of tools under
the moniker of Governance, Risk and Compliance (GRC). This chapter 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?

2 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 dif-
ferent disciplines focus on risk as it applies to them. From the IT security per-
spective, 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 exercising a par-
ticular potential vulnerability and the resulting impact of that adverse event on
the organization [1].

2.1 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 Publica-
tion (SP) 800-30, Risk 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 [2].

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

The threat is merely the potential for the exercise of a particular vulnerabil-
ity. 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 differ-
ent 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.
2.2 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

<table>
<thead>
<tr>
<th>Threat (including threat-source)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental disclosure</td>
<td>The unauthorized or accidental release of classified, personal or sensitive information</td>
</tr>
<tr>
<td>Acts of nature</td>
<td>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</td>
</tr>
<tr>
<td>Alteration of software</td>
<td>An intentional modification, insertion or 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</td>
</tr>
<tr>
<td>Bandwidth usage</td>
<td>The accidental or intentional use of communications bandwidth for other than intended purposes</td>
</tr>
<tr>
<td>Electrical interference/ disruption</td>
<td>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)</td>
</tr>
<tr>
<td>Intentional alteration of data</td>
<td>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</td>
</tr>
<tr>
<td>System configuration error (accidental)</td>
<td>An accidental configuration error during the initial installation or upgrade of hardware, software, communication equipment or operational environment</td>
</tr>
<tr>
<td>Telecommunication malfunction/ interruption</td>
<td>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</td>
</tr>
</tbody>
</table>
or intentionally exploited) and result in a security breach or a violation of the system's security policy [3].

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

3 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.

4 Managing risk at the organizational level

Before you can manage risk at the IT system level, you have to be able to manage risks at the organizational level. Risk related to the operation and use of information systems is another component of organizational risk that senior leaders must address as a routine part of their ongoing risk management responsibilities. Organizational risk can include many types of risk (e.g., investment risk, budgetary risk, program management risk, legal liability risk, safety risk, inventory risk and the risk from information systems) [4].
Deciding upon the acceptable level of risk for the organization, sometimes called the risk tolerance, is the responsibility of upper management. While upper management needs to be advised on IT security risks by a specialist, the actual decision should always be made by upper management.

NIST defines a Risk Executive function that ensures risk decisions are made from an organizational perspective keeping in mind the mission and business functions. This function can be of one or more individuals who interact with senior management and IT security specialists to provide a holistic view of tolerable risk that will allow the organization to fulfil its mission in a cost-effective manner.

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

Recall that threat is a potential likelihood that something bad will happen. This has historically proved very difficult to measure. The most meaningful data are statistics collected directly by the organization. If this is not available, there are some high-level indicators of likelihood that have been collected across the industry. The Consensus Audit Guidelines (CAG) identifies the top 20 effective controls. Since controls are applied against risks, the likelihood component can be inferred. While this does not give a concrete picture of likelihood, it does allow the organization to focus on the top observed risks. The CAG is based on the observed effectiveness of various security controls in preventing compromise. The CAG was developed by the Center for Strategic and International Studies, which included numerous U.S. government agencies along with experts from the banking and critical infrastructure communities.

Vulnerability is much easier to measure. It is the impact on the business if a particular weakness is exploited. For those vulnerabilities where the impact is very clear, the impact can be measured consistently. However, other vulnerabilities can have a range of impacts, from a minor annoyance to completely compromising the entire system. For these vulnerabilities, there are two basic schools of thought: prepare for the absolute worst case or prepare for the worst reasonable case. Both these approaches have their pros and cons. Absolute worst case may overstate the impact for a particular vulnerability, while worst reasonable case relies heavily on likelihood.

In addition, the reader is directed to read the U.S. Department of Commerce’s, National Institute of Standards and Technology Interagency Report 7564, Directions in Security Metrics Research for an in-depth discussion on security metrics (http://www.nist.gov/customcf/get_pdf.cfm?pub_id=902180).
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 and so on, 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 1-year period.

\[ ALE = SLE \times ARO, \]

where

- Single Loss Expectancy (SLE) 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.
- Annualized Rate of Occurrence (ARO) is how often the loss occurs. This is the likelihood.

While utilizing quantitative risk assessment seems straightforward and logical, there are issues with using this approach with information systems. This previous discussion highlighted the difficulty of getting an accurate value for likelihood (i.e., ARO). Moreover, although the cost of a system may be easy to define, the indirect costs, such as the value of the information, lost production activity and the cost to recover, may be more difficult to determine.

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.

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 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 [5].

Currently, the relative difficulty of obtaining accurate and complete information limits the usage of quantitative risk assessments in IT security. Nonetheless, if the information is deemed reliable, a qualitative risk assessment is an extremely powerful tool to communicate risk to all levels of management.

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 define 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.

In a qualitative risk assessment, it is best not to use numbers when assessing risk. Managers, especially the senior-level managers who 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.

**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 the following:

- 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 Table 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.

A best practice is 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.
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 websites and public vulnerability archives, National Vulnerability Database or NVD (http://nvd.nist.gov).

NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement and compliance. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names and impact metrics [6].

If they exist, previous risk assessments and audit reports are the best place to start to identify vulnerabilities.

Moreover, 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, COBIT or NIST SP 800-53) 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.

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 dis-
covered and that the T-V pairs would change fairly often.

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

**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.

Be very careful in setting up the likelihood definitions. Table 2 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.

**Defining impact**

In order to ensure repeatability, impact is best defined in terms of impact upon
availability, impact upon integrity and impact upon confidentiality. Table 3
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. Table 4 shows these specific values.

<table>
<thead>
<tr>
<th>Definition</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0–25% chance of successful exercise of threat during a 1-year period</td>
<td>26–75% chance of successful exercise of threat during a 1-year period</td>
<td>76–100% chance of successful exercise of threat during a 1-year period</td>
</tr>
</tbody>
</table>

Table 2: Sample likelihood definitions
Critical Infrastructure Security

It is vital to apply the impact definitions across the entire organization. In order to effect this, ensure that these definitions are supported by the Risk Executive function in the organization.

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

---

Table 3: Sample impact definitions

<table>
<thead>
<tr>
<th>Level</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Loss of confidentiality leads to a limited effect on the organization</td>
<td>Loss of integrity leads to a limited effect on the organization</td>
<td>Loss of availability leads to a limited effect on the organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Loss of confidentiality leads to a serious effect on the organization</td>
<td>Loss of integrity leads to a serious effect on the organization</td>
<td>Loss of availability leads to a serious effect on the organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Loss of confidentiality leads to a severe effect on the organization</td>
<td>Loss of integrity leads to a severe effect on the organization</td>
<td>Loss of availability leads to a severe effect on the organization</td>
</tr>
</tbody>
</table>

Table 4: Examples of organizational effect

<table>
<thead>
<tr>
<th>Effect type</th>
<th>Effect on mission capability</th>
<th>Financial loss/damage to organizational assets</th>
<th>Effect on human life</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited effect</td>
<td>Temporary loss of one or more minor mission capabilities</td>
<td>Under $5,000</td>
<td>Minor harm (e.g., cuts and scrapes)</td>
</tr>
<tr>
<td>Serious effect</td>
<td>Long-term loss of one or more minor or temporary loss of one or more primary mission capabilities</td>
<td>$5,000–$100,000</td>
<td>Significant harm but not life threatening</td>
</tr>
<tr>
<td>Severe effect</td>
<td>Long-term loss of one or more primary mission capabilities</td>
<td>Over $100,000</td>
<td>Loss of life or life threatening injury</td>
</tr>
</tbody>
</table>
take any planned controls into consideration. Table 5 can be used to evaluate the risk when using a three-level rating system.

Following this logic, if likelihood and impact were evaluated on a Low, Moderate, High basis, risk would also be Low, Moderate or High.

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.

6.1 Strategies for managing individual risks

There are four basic strategies for managing risk: mitigation, transference, acceptance and avoidance. Each will be discussed below.

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.

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.
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.

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.

6.2 High-level risk management strategies
Managing every risk on an individual basis is costly and time consuming. Instead, focus on strategies to manage all the risks associated with the organization’s IT systems rather than on the individual risks.

Managing risk using baselines
Continuing with the theme of measuring and managing risk in a consistent and repeatable manner, an organization should develop a baseline set of controls that will reduce risk to an acceptable level. However, not all information and business processes are equally valuable to the organization. As discussed earlier, organizational value of information and business processes is measured by the impact on the organization where the information or business process to be compromised. Therefore most organizations develop multiple baselines, corresponding to the different impact levels. NIST SP 800-53 defines three baselines corresponding to Low, Moderate and High impact.

The most effective risk management technique is avoidance. Requiring systems to comply with a baseline does not require tremendous analysis to determine if a system will operate at an acceptable level of risk. However, not all systems can implement every control in the baseline. In these cases, the experts must come together and analyse the situation, either establishing compensating controls or using one of the other three risk strategies, and grant an exception. Exceptions generally require greater resources (due to the additional analysis) but allow flexibility.
So manage risk by compliance where possible and by exception where necessary.

**Using threat zones**
Threat zones are a tool that can be used to tailor existing baselines to take into account attacks on certain systems are more likely. Attacks can be more likely due to the system placement. (Internet facing systems are subject to more frequent attacks than intranet servers that are not directly accessible from the Internet.) By defining threat zones and associating additional controls to systems within the threat zones, the systems can operate at a tolerable level of risk. While these additional controls could be added to the baseline, it might not be cost effective to deploy the controls for all systems in the entire enterprise (e.g., write-only logs).

**Managing risk prior to deployment**
Before deployment is the optimal time to reduce risk to the lowest level. Applying the baseline controls during development is typically orders of magnitude less costly as well as generally being more effective than building in additional controls after deployment.

The often maligned certification and accreditation process is merely testing the controls required by the baseline and a formal acceptance of risk by appropriate management. By including the baseline in the system requirements, implementing the baseline during the design/development/integration and testing the controls, systems with a set tolerance for known risk can be deployed.

This same process should be utilized for any additions or changes to the system before they are deployed.

**Managing risk after deployment**
After deployment, periodic exhaustive retesting of all the baseline controls has shown to be largely ineffective. Continuous monitoring of the system is the strategy that has proven to be most effective at managing risk. Continuous monitoring is the process of monitoring known attack vectors and operational processes that have been known to fail. Reviewing logs, patching the operating system and auditing account management are among the more effective continuous monitoring targets. The CAG is widely considered the seminal set of continuous monitoring targets.

### 6.3 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 present risk in a way they will understand. Do not use ‘fear, uncertainty and doubt’. Instead, present risk in terms of likelihood and impact. Organizational management will more
readily understand and accept the findings and recommendations based on consistent terms rooted in facts.

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 strategy is showing the residual risk after the risk management strategy was enacted (Table 6).

### 6.4 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.
Table 7: Sample POAM

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Management Strategy</th>
<th>POC</th>
<th>Resources Required</th>
<th>Milestones</th>
<th>Target Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure in environmental systems (e.g., air conditioning) leaves systems unavailable</td>
<td>Implement a hot spare at the alternate site</td>
<td>Joe Smith</td>
<td>$100,000 hardware</td>
<td>Procure hardware &amp; software</td>
<td>9/1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$50,000 software</td>
<td>Install hardware</td>
<td>9/15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$100,000 labour</td>
<td>Install software</td>
<td>10/1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Configure system</td>
<td>10/15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Test system</td>
<td>11/1</td>
</tr>
</tbody>
</table>

Table 7 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 is listed. Note that the POAM is a tool to communicate to management, rather than a project management plan.

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.

7.1 NIST methodology

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, is the U.S. 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 comprehensive, covering everything from threat-source identification to ongoing evaluation and assessment.

The NIST methodology consists of nine 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 2 gathers knowledge from operational area managers. Phase 3 gathers knowledge from staff and develops the protection strategy.

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 Peltier Associates, teach FRAP.

7.4 GRC tools

Over the last few years, GRC tools have exploded onto the marketplace. Driven by government and statutory requirements these tools are capable of tracking compliance against standard and custom baselines. Moreover, some of these tools can directly measure compliance (SCAP is becoming more prevalent) and even enforce baselines.

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.

References


