

Risk Assessment and Compliance

A Management Tool for the IT Security Infrastructure

By

Caroline Ramsey Hamilton

Background

Since the collapse of Enron in December 2001, corporations have been under increasing scrutiny by government regulators who want to ensure that investors are protected, that individual medical records are protected and that online banking offers a safe environment for consumers.

Many of these new requirements include a risk assessment component as part of the compliance activities. The assessment component of the risk assessment is also being used as a way to validate compliance with other sections of IT security regulations such as the FFIEC Examination Handbook, Bank Secrecy Act revision of 2006, Gramm Leach Bliley Act, the HIPAA Rule, Cobit IV and the Sarbanes Oxley Act.

These new regulations require more stringent security and other requirements that influence the nature of both information security and physical security. These new requirements are mandatory -- and most are subject to either audit or review, by an outside organization. Many of these requirements are listed in Figure A1 (below). A key element in these requirements is the risk analysis/risk assessment requirement (also called a self assessment), that forces organizations to conduct a formal assessment of their IT security infrastructure including:

- ❖ the threats that are present
- ❖ the assets that need protection
- ❖ a review of existing vulnerabilities
- ❖ an analysis of these elements, such as threat/vulnerability pairing
- ❖ culminating in a list of controls that will be implemented.

According to the FFIEC (Federal Financial Institutions Examiners Council) IT Handbook, “**Information security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems. An adequate assessment identifies the value and sensitivity of information and system components and then balances that knowledge with the exposure from threats and vulnerabilities. A risk assessment is a necessary prerequisite to the formation of strategies that guide the institution as it develops, implements, tests, and maintains its information systems security posture. An initial**

risk assessment may involve a significant onetime effort, but the risk assessment process should be an ongoing part of the information security program.

The Sarbanes-Oxley Act

Without a doubt, the Sarbanes-Oxley Act (SOX) is the single most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s. And, it is clear that public companies and the accounting profession have made tremendous progress in meeting the rigorous requirements of this legislation. Risk Assessments or self-assessment using risk-based gap analysis techniques help organizations discover where they are in their SOX compliance.

WHAT IS A RISK ASSESSMENT ?

Risk assessment is the cornerstone of security. Risk assessment looks at a variety of threats:

- both internal and external
- considers the value of the organizational assets, such as consumer information, including dependencies
- calculates a risk rating, as well as recommending solutions that are prioritized by Return On Investment.

The risk assessment process includes gathering information about the assets of the organizations, including all information assets such as networks, data centers, computers, hardware, software, data/information; and all physical assets, such as the personnel who staff the organization, the integrated systems, the physical facility and dozens of other organizational resources. In addition, the risk assessment process includes finding sources for threat data, which may be gathered from internal sources such as incident reports and intrusion detection reports. It may also include threat data such as crime statistics, industry standards and benchmarking data, and historical data about what has happened in the organization, and in the general industry segment.

Risk assessment is a method of determining what kind of controls are needed to protect an organization's assets and resources not just adequately, but also cost-effectively. The risk assessment process analyzes a set of five variables, and comes up with recommended actions based on the relationships of these variables to each other and how compliant the organization is with existing requirements

WHY SECURITY COMPLIANCE IS CRITICAL TO RISK MANAGEMENT

To properly assess an organization, an information system, a operation, or a facility, it is necessary to have something to measure against. There has to be a baseline security standard and in the past, it was hard to find a universal standard for security.

The plethora of new requirements, especially the ISO-IEC 17799-2005 and ISO 27001 for Information Security Management, and the many new requirements covering the handling of consumer information encourage organizations to have more uniform and up-to-date assessments and also allow the possibility of benchmarking for global organizations that do business internationally. There is a tremendous value for large

organizations to be able to measure against recognized standards that allows them to compare different business units, different systems, or different facilities within the organization. There is also great value in having an auditable process that allows an organization to prove that it has done the required assessments. Risk assessment is a management process and, by its nature, should involve the whole organization.

Employees must be an integral part of the risk assessment process. Employees see security from a different and very valuable perspective -- they integrate it into their daily work. Whether you are going to include network or systems users; or whether you are going to be looking for answers from production workers, supervisors or the shipping and receiving clerks, getting information from a wide variety of individuals is extremely important to the validity and accuracy of the risk assessment.

In order to make it easy to involve others in the organization, management involvement from the very beginning can make the difference between a successful risk assessment and one that is difficult to complete, with the final results possibly questioned or disregarded. The key to obtaining strong organizational support for the risk assessment includes the following elements:

- **Getting Management Buy-In**
- **Involving the Entire Organization**
- **Asking Good Questions - Developing the Survey**
- **Structuring an Effective Project Plan**

MANAGEMENT BUY-IN FOR THE RISK ASSESSMENT

If you are conducting a risk assessment, it means that the activity AND the budget for risk assessment have already been approved by management, whether you are in-house staff, or an outside contractor. However, just having the go ahead for a risk assessment is not enough. You will need management support from the top of the organization to be able to do an effective assessment.

As the risk assessor, you should request that senior management write an email or memo to the entire organization, explaining that a risk assessment will be starting soon. The higher in the organization you go for support, the better your results are going to be. Whether it's the CEO, COO or CIO, a Vice President or a Director, it's important to show that you have top level support for the assessment. This will create an atmosphere where people will be more helpful and you will have less trouble finding the information you need, and it will also have an influence on how the final results of your assessment are received.

Senior management may not have much information about how the risk assessment works and it will be your job to educate them so they understand the critical role of risk assessment in the organization. Often, relating stories of security problems at

other organizations and including media reports creates an appreciation for the role risk assessment can play within an organization.

INVOLVING THE ORGANIZATION IN THE ASSESSMENT

In structuring the risk assessment, it will be necessary to gather information from individuals in various parts of the organization. The risk analysis manager is the analyst in charge. According to the audit guidelines for risk assessment, the more people you interview, the more likely you are to find a vulnerability. Individuals should not be asked to answer more than 50-100 questions, which are directly related to their job. For example, a network user might answer questions related to whether they use their passwords, whether they log off their terminals when they leave their station, or whether they have attended basic data security training.

To gauge how well individuals within the organization are complying with the organization's security practices, it is important to receive input from a wide variety of individuals, including people who work in different parts of the organization, different business units, different facilities and different shifts in the same facilities. It is a good idea to have a representative of each area involved in the structuring of the risk assessment because they can suggest individuals who might answer questions, and they can also help by making sure that each survey or interview is completed in a timely manner.

These individuals become part of the risk analysis team. Team members will review questions, identify the appropriate standards for their areas, assist the risk analyst in arriving at current asset replacement values, and serve as administrative support for the surveys in their respective areas of responsibility

ASKING GOOD QUESTIONS

Asking good questions is the very heart of the risk assessment and also forms the core of the vulnerability assessment. Questions should be set up to validate compliance against published policies, guidelines and directives. If you ask questions that are not linked to standards, and discover major problems, the path will not exist to force compliance. Limiting the number of questions to ask is one of the most difficult aspects of the analysis.

It is unrealistic to think that people will answer more than fifty to one hundred questions. To avoid individuals having to answer questions that do not relate to their area, in a risk assessment, questions are divided into job categories, or what is called 'functional areas.' Functional areas are pieces of a job. By dividing up questions into these categories, for example, Michael Smith may answer 20 questions for network users, 20 questions for personnel management (which is his area), and 15 general organization questions. More specialized personnel, such as facilities managers, the physical security officer, or a database administrator will answer questions that relate only to his/her particular area.

THE ANALYSIS

The most difficult part of a risk assessment is the actual analysis. There can be more than five million potential combinations of just 25 asset categories, 38 threat categories, 7 loss categories, 40 vulnerability categories and 200 potential safeguards (controls). So the analytics involved in analyzing the collected information is a major element of the assessment and those analytics are used to produce the final report.

A report should include:

- Asset information
- Threat matrixes
- Compliance and vulnerability graphs (see below)
- The loss impact projections
- And the controls recommended by their Return On Investment.

The cost benefit analysis combines information from:

- a. the vulnerability assessment
- b. the relevant threat data and asset information such as present day replacement values and criticality
- c. and how completely safeguards are currently being implemented.

In reviewing the existing security controls, it's important to indicate percentages of current implementation. For example, maybe the visitor badging policy is only 70% implemented, meaning that it is implemented on weekdays, but not on weekends.

RETURN ON INVESTMENT

Many new security funding initiatives look at the total security profile of an organization, and, using a risk assessment process, prioritize the potential security expenditures by their Return On Investment, that is, which new safeguards provide the 'most bang for the buck'. How else does an organization decide whether to implement personnel screening procedures, or hire additional guards, or invest in a managed service to protect their networks?

The cost benefit analysis combines information from the vulnerability assessment along with relevant threat data and asset information such as present day replacement values, criticality, integrity and availability of the information contained in the system under review, as well as how completely safeguards are currently being implemented. The result of the cost benefit analysis will be to create a return on investment (ROI) ratio, balancing the value of the information against the cost of controls to protect it. By establishing Return On Investment data, managers and directors can strengthen their security budgets, and make more informed decisions regarding which controls to implement, based not strictly on initial cost, but also on the current threat exposure of the organization or the industry.

In actual risk assessments, completing implementation of an existing control to 100% is often the most cost effective solution. The result of the cost benefit analysis would be to

create a return on investment ratio (ROI), balancing the value of the information against the cost of controls to protect it. By establishing Return On Investment data, managers and directors can make more informed decisions regarding which controls to implement, based strictly on initial cost, but also on the current threat exposure of the organization.

Basing security controls on Return On Investment takes the risk and compliance assessment to a new level. It is a method of looking across a large organization in a consistent and quantifiable manner, with defensible, auditable results. It also provides a way of benchmarking the effectiveness of security throughout an organization and it will identify the weak areas so those can be revisited with a more intensive analysis at a later date.

Accountability, which is a built-in component of risk assessment, is increasingly important to senior management. Board members and shareholders see the value in using quantitative numbers to assess the security level of an organization and support the resulting management recommendations. As corporate security policies and compliance regulations are created to address the increasingly regulated compliance environment, security risk management in general, and automated software for risk analysis in particular is becoming an increasingly important tool in corporate governance.

Caroline R. Hamilton is an expert in security and compliance risk assessment and President of RiskWatch, Inc., a company specializing in security risk assessment software. She was a Charter member of the National Institute of Standards and Technology's Risk Management Model Builders Workshop, which was a joint Workshop between U.S., Canada and the United Kingdom to create the first security risk management guidelines from 1988 – 1995. In 1996, she served on the U.S. National Security Agency's Network Rating Model workshop, and from 1996-1998,

served on the working group to create a Defensive Information Warfare Risk Management Model, for the U.S. Department of Defense, under the auspices of the Office of the Secretary of Defense.

She is a member of the IBM Data Governance Council and is currently writing a book on Risk Analysis/Risk Assessment for Elsevier Publishing. She has been published in The Computer Security Journal, Security Management Magazine, Business Week, Security Technology and Design, the CSI Alert, Defense Electronics and Access Control . She is a graduate of the University of California, Riverside and lives near Davidsonville, Maryland.