Risk Management, Security Compliance and Audit Controls

This chapter includes:

- Risk Analysis
- Risk Assessment
- Business Impact Analysis
- Defense in Depth Model
- Data Classification
- Risk Management
- Compliance and Audit Controls
- FMECA Fault Trees
- Event Trees
- CCA
- TBA

Introduction

In this chapter we introduce the major methods used in risk measurement and audit. Security risk assessment is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. First we will look at defining risk and the terms; next we will look at a few of the methods used.

What is a process?

Processes are the methods that we used to achieve our objectives. How are processes implemented within an organization?

Objectives

An objective is a goal or something that you wish to accomplish. Who sets objectives and how are these designed to help achieve effective risk management?

Controls

Controls are the mechanisms through which we reach our goals, but what are controls? Controls are useless if they are not effective so we need to ensure that any control is effective and may be justified in cost terms. This is one of the main purposes of an audit.

Controls are the countermeasures for vulnerabilities. There are four types:

- Deterrent controls reduce the likelihood of a deliberate attack
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventative or corrective controls.

Policies

Policies are themselves controls. Every policy in the organization should relate to a business or organizational objective. What you need to ask is who sets policy and how? Some of the other questions to ask include:

- What practices are employed?
- How does our organization ensure that the practices are what is in effect?
- Policies and practices should match, how is this checked?
- When a practice doesn't match. There is an issue – how do issues get resolved?

System

A system is defined in NIST (800-30) as any collection of processes, and/or devices that accomplishes an objective. The auditor needs to have a comprehensive understanding of systems design and testing.

Identifying classify risk.

A risk analysis is a process that consists of numerous stages. Become familiar with each of these processes and you will be able to conduct the following:

- Threat analysis, how is a threat determined.
- Vulnerability analysis, what is a vulnerability.
- Business impact analysis, how will an event impact the organization's business?
- Likelihood analysis, what is the probability of an event.
- How are these individual components merged in order to deliver the overall risk rating for an organization and what does that mean?

The Risk analysis process should allow the organization to determine the risk for an organization based on threats and vulnerabilities. From this point, the auditor will be able to classify the severity of the risk and thus assign an overall importance to each risk. It should be feasible to use this information to create a risk management plan (SANS, 2005). This should consist of:

- Preparing a risk treatment plan using a variety of control methods.
- Analyzing individual risks based on the impact of the threats and vulnerabilities that have been identified from the risks.
- Rate the individual risks from highest to lowest importance.
- Create a risk treatment plan that categorizes each of the threats and vulnerabilities in order of its priority to the organization, together with some possible controls.

An example risk treatment matrix as listed below (as modeled from NIST (800-42) and Microsoft (2004)) should be well within any organizations capability to create following this process.

No.	Threat/Risk	Priority	Controls						
			Policy	Procedure	Firewall	IDS	Av	etc	
1	Unauthorized access to application and internal networks and	H	*	*	*				
2	data integrity	H							
3	Unauthorized transmission of confidential information	H							
4	Data corruption	H							
5	Spoofing	M							

Implementing a risk mitigation strategy

The auditor must understand what is required for a Gap analysis, and how this allows the identification of controls that have not been implemented. Threat modeling and development of attack trees help to develop a competence, which will allow the auditor or security professional to decide whether each gap from the gap analysis should be either excepted or mitigated and what type of controls.

Plan do check act

Originally implemented as a quality control process, ISO 17799 (ISO 17799.2) has adopted the plan, two, check, act methodology. The auditor should be aware of this process. This process involves the following stages (Six Sigma[1]):

Plan

The plan phase consists of an identification of the problem, followed by an analysis of the problem identified. The key components of this phase include threat and vulnerability analysis.

Do

The next phase of the PDCA process requires the development and implementation of ISMS (information security management system) components. This would include controls. The auditor should understand the various types are controls, and why they are chosen.

Check

The check phase consists of an evaluation of the previously implemented ISMS components for controls. Although audit is a control in itself, it should also be used to measure effectiveness of the overall process and its components.

Act

Finally, the act phase of a PDCA based process requires that the organization continuously improve its performance. Using constant incremental improvements, the organization should be old to consistently improve its security systems minimizing risk while remaining cost-effective.

Risk management, security compliance and audit controls

What makes up a risk program?

In order to answer this question it is necessary to understand how to identify and quantify the effectiveness and cost of the various risk analysis techniques. You must understand the risk management process as a whole, and how controls may be implemented to eliminate or mitigate the risk of individual events occurring.

Security compliance has become a major factor in driving risk processes within business and government. An understanding of the security controls and measurement techniques, audit controls and processes used to ensure that the controls work within a system is crucial. This should lead to an introduction to the discipline of governance, as it relates to Information Systems.

Risk analysis: techniques and methods

1 http://www.sixsigma.com

The auditor needs to be introduced to a variety of risk methods. The chapter covers some of the key methods below.

Overview of Risk Methods

- General types of risk analysis
- FMECA
- CCA
- Risk Dynamics
- Time Based
- Monte Carlo
- Some Tools

General risk analysis

Risk analysis is the art and science of determining the real and potential value of an asset, while simultaneously attempting to predict the likelihood of loss based on mitigating security controls [NIST (800-30) and Bosworth, 2002].

Risk analysis models

There are two basic forms of risk analysis:

- Qualitative
- Quantitative

Quantitative analysis will be based on object of data analyzing the sufficiency of controls, and uses some numerical method.
Qualitative is designed to analyze the quality of the system from a subjective point of view.
The auditor must know the differences between these models, the benefits of each end of the downside to selecting either type of risk model.

Quantitative

The two simple models of quantitative risk that all auditors and risk professionals must know:

- Annualized loss.
- Likelihood of loss

In addition, the auditor should understand that there are other quantitative methods. Some of these methods are detailed later in this chapter and should be included as a minimum. Though it is not expected that the auditor would learn all of these advanced techniques, they should know of their existence.

The probability of an event occurring and the likely loss should it occur are the two fundamental elements of the quantitative method.

Quantitative risk analysis makes use of a single figure produced from these elements. Called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)', this is calculated for an event by simply multiplying the potential loss by the probability.

It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this. The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability is rarely very precise. This often promotes complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.

Placing a value on Risk Management

Internal Value

Internal values consist of a monetary value associated with the organizations asset. Some of the following are examples of factors which influence the internal value of an asset;

1. Time required to retrieve lost information (i.e. from backup),
2. The labor costs associated with –
    a. Creating the system initially,
    b. Rebuilding the system ,
    c. Lost or effected productivity,
3. Costs (labor, maintenance etc costs) associated with the continued operation of a system (e.g. patching activities).

External Value

This refers to the value that the resource brings the organization from external sources. This is usually a value that is easy to quantify as it is an amount generated from the system. Accounting records will often separate resources for reporting purposes. A business case to justify the system should also have the external values detailed.

Total Value

Total Value = Internal Values + External Values +TCO

Where an asset is dedicated to a specific task (i.e. external commerce server) the total value is easy to calculate. If there is a dual use this may be difficult (e.g. a Web Server that provides both extranet services for clients and an Intranet function).

ALE – Annualized loss Expectancy

ALE is a calculation which is designed to help formulate the expected potential loss from perceived threats and impacts (see above). The ALE is used as a tool to prioritize protections on an organizations asset.

ALE = SLE *ARO

EF – Exposure Factor (or likelihood factor)

EF is defined as the expected percentage loss to an asset from a particular defined threat. This is basically an educated guess.

SLE – Single Loss Expectancy

SLE is calculated as an asset total value multiplied by an exposure factor (or likelihood factor). The total value of the asset is defined as its individual TCO (see above).

SLE = TCO x EF

ARO – Annualized Rate of Occurrence

ARO is the expected rate of which a threat may occur in a given year. This value is an educated guess. Technical staff can probably judge better than business staff what the likelihood of a threat occurring is in the security arena.

Qualitative Risk

Qualitative analysis is the easiest type analysis, but the results are easily skewed by personal opinion. These methods are typically focused on measuring or estimating threat and vulnerability. Qualitative analysis is the simplest and cheapest method of analyzing risk, but should never be forgotten that perception is not always accurate end of the results are based on guesswork.

This is by far the most widely used approach to risk analysis. Educated guessing of probability based data is not required and only estimated potential loss is used.

Threats + impact + likelihood = risk

Before deciding how to protect a system, it is necessary to know what the system is to be protected against i.e. what threats are to be countered. In the following sections different types of threats are presented.

Threats are divided up into the following categories:

- General, Identification / Authentication,
- Availability, Privacy,
- Integrity / Accuracy,
- Access Control,
- Repudiation,
- Legal.

In this section of the analysis a table is presented containing:

- The threat (including description),
- the impact of the threat (a reference to the impact table),
- plus a number (0-5) and
- the likelihood of the threat occurring (number 0-5).

Most qualitative risk analysis methodologies make use of a number of interrelated elements.

Threats

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are present for every system.

Threat Sources

The following are just some of the many threats that may affect your organization:

1. Political espionage.
2. Commercial espionage. Since the end of the cold war, the entire intelligence community has undergone a significant shift from classical east-against-west spying to each-country-must-protect-its-economy. Former KGB and CIA employees are now working as freelance commercial intelligence services. Sources of such espionage are competitors (domestic and international).
3. Employees:
   - Disgruntled employees and (former) employees.
   - Bribed employees.
   - Dishonest employees (possible at all levels: from top management down).
   - System & security administrators are "high-risk" users because of the confidence required in them. Choose with care.
4. Organized crime (with goals such as blackmail, extortion etc.).
5. Private investigators, "mercenaries", "free lancers".
6. Law enforcement & government agencies (local, national and international), who may or may not be correctly following legal procedures.
7. Journalists looking for a good story.
8. Hackers:
   - Beginners: know very little, use old, known attack methods (aka script kiddies)

- Braggers: Are learning a lot, especially from other hackers. They seek gratification by bragging about their achievements
- Experts: High knowledgeable, self reliant, inventive, try to be invisible. They may provide tools/information to the braggers to launch attacks, which hide their own, more subtle attacks.

9. Contractors / vendors who have access (physical or network) to the systems.

Vulnerabilities

These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, in the case of a fire vulnerability, the presence of inflammable materials (e.g. fuel) is a threat.

FMECA analysis

MIL-STD-1629 Procedures for Performing a Failure Mode, Effects and Criticality Analysis should be understood in detail. Failure mode, effects and criticality analysis helps to identify:

- Risk factors,
- Preventative controls.
- Corrective controls

FMECA couples business continuity planning or disaster recovery into the initial analysis

- identifies potential failures
- identifies the worst case for all failures
- occurrence and effects of failure are reduced through additional controls

The FMECA Process consists of the following stages:

1 Define the system or target

a. What is the systems mission?

b. How does the system interface with other systems?

c. What expectations for example, performance and reliability affect the system

2 Create a block diagrams

a. FMECA relies on the creation of block diagrams

b. Diagrams illustrate all functional entities, and how the information flows between them.

3 Identify all possible individual modules system failures and system interface failures:

   a. Every block in every line that connects the block is a potential point of failure.

   b. Identify how each failure would affect the overall mission of the system

4 Analyze each possible failure in a terms of a worst-case scenario.

   a. Determine a severity level for the failure.

   b. Assign this value to the possible outcome.

5 Identify,

   a. Mechanisms for detecting failures.

   b. Compensating controls relating to the failures.

6 Create describe any actions necessary to prevent or eliminate the failure or effects of the failure

   a. the Define additional, setting controls to prevent or detect the failure

7 Analyze and describe any and all effects of the additional controls

   a. define the roles and responsibilities to address the compensating controls

8 Document the analysis

   a. Explain the problems found in the solutions.

   b. Document residual risks -i.e. days without compensating controls.

   c. Describe the potential impact of these residual risks.

FMECA summary

This process involves a detailed analysis based on qualitative methods. It is reasonably objective, helps to identifies controls and issues and also identifies residual risk.

CCA - cause consequence analysis

RISO labs (Riso National Laboratory: 307-312) developed CCA (Cause consequence analysis) which is essentially a fault tree based approach. It is commonly used for analysis of security and safety problems. CCA and fault trees can be easily applied to almost any technology or system.

The tree based approach involves the following steps:

- Identify an event

- Determine the underlying causes of the event.
- For each underlying cause identify the causes or initiating events.
- Repeat until the underlying cause becomes uncontrollable

The CCA process is repeated until the final underlying cause is beyond the organization's control (whether through cost or other factors). Thus the process ends when there is no value in continuing to decompose the problem further.

Two tree types

- Fault trees
  - Identify faults
  - Determine underlying causes of the faults
- Event trees
  - Identify faults.
  - Identify consequences

CCA combines both fault trees and event trees. As a result, CCA is good for incident handling analysis, both pre-and post-incident. This helps us to determine how an actual incident may occur. CCA is commonly used as a form of qualitative analysis for determining possible failures. Auditors should be able to create and analyze fault and event trees in order to diagnose organizational risks.

Risk dynamics

Risk dynamics looks at risk analysis and risk mitigation, as in equilibrium. Thus, making a change to any control or other risk factor will impact another term. Some risk dynamic terms include:

- cost to secure
- level of threat
- severity of the vulnerability
- the impact and consequences of any exposure
- time to detect an incident
- the time to respond to an incident
- recovery time
- the overall risk

Risk dynamics is a qualitative approach to risk that uses the formula:

Threat X Vulnerability = Risk

Auditors should understand this methodology, its weaknesses and its benefits. They should understand the processes and stages involved with this methodology.

Time-based Analysis (TBA)

Time-based analysis is a quantitative analysis that uses only a small amount of qualitative measures. TBA is extremely effective in measuring the adequacy of a control. This is also useful in terms of fault preparation.

TBA involves analysis of the systems to identify:

- The preventative controls (P)
- The detective controls (D)
- And the reactive controls on the system (R)

TBA measures all things in terms of time. As long as the time to detect and react to an incident is less than the amount of time to prevent the fault risk is maintained at an acceptable level.

Thus, the aim when implementing TBA is to maintain the following situation:

D + R < P

And a measurable loss occurs when:

D + R > P

To analyze controls under a TBA, first assume that preventative controls fail then asked the questions:

- How long does it take for detective controls to be enacted?
- How long following detection, does it take for a response to be initiated?

The aims of a TBA based risk strategy include reducing both D & R. this can be achieved by improving the detective controls or improving the reactive controls. The TBA model assumes that all preventative controls will eventually fail given enough time (SANS, 2005).

In determining a target, the costs of the preventative, detective and reactive controls are taken into account to create a cost benefit analysis. TBA is one of the simpler quantitative methods of risk analysis and management that is available. All auditors should be familiar with this methodology.

Monte Carlo method

A number of stochastic techniques have been developed to aid in the risk management process. These are based on complex mathematical models that use stochastically generated random values to compute likelihood and other ratios for our analysis model.

The Monte Carlo method can also aid in other risk methodologies such as Time-based analysis (Curtis, et al 2001). It further allows me determination of the range of possible outcomes and delivers a normalized distribution of probabilities for likelihood. Combining stochastic techniques with Bayesian probability and complex time series analysis techniques such as Heteroscedastic mapping is mathematically complex, but can aid in situations where accuracy is crucial.

These methods are truly quantitative. They help predict any realistic detection, response and thus exposure time. This may be differentiated by the type of attack. This type of statistical method is to have a downside in that they are more expensive than the other methods. The level of knowledge needed to conduct this type of analysis is not readily available and the level of knowledge of the organization needed by the analyst often excludes using an external consultant in all but the smallest of risk analysis engagements.

Some existing tools for risk analysis

Selection of the common tools available should be introduced to the auditor. Some of the more common tools that may be introduced to the auditor are included below.

Crystal ball

Crystal ball is a simple Monte Carlo simulation/analysis product. It uses tornado analysis and life in hyper acute sampling. Crystal ball is one of the simpler stochastic risk analysis tools available.

Risk +

Risk + is designed for performing schedule risk analysis. It is a simple time based analysis system used to identify potential faults in a fault tree style. Risk + uses Monte Carlo simulations to determine likelihood. This enables the product to demonstrate a possible cost by using the resource allocation values that it has created through cost histogram. This probability histogram is based on stochastically determined outcomes.

Cobra

Cobra is particularly useful for organizations that use ISO 17799 as a security model. It is used to measure the ISMS of the organization against the 10 core controls of ISO 17799. Cobra uses a cost justification model based on cost benefit analysis. Cobra integrates they risk dynamics based approach to knowledge-based questionnaires.

OCTAVE

As one of the leading risk methodologies, Octave should be explored. It would not be expected that an auditor should understand the process in its entirety, but they should know the fundamentals of how this process works and what its benefits, and downsides are.

Creating a Information Systems Risk Program

The objectives of any information risk program should need to introduce the organizations to arrange of risk assessment models and also give management something to use right away. Some of the key skills and that should be transferred to management in a risk program include the following key areas which have been defined to be the core components of a risk management process:

- Being able to competently conduct an information security risk assessment,
- Having a basic understanding and the required knowledge to Perform asset identification and classification for a basic organization,
- Perform threat identification and understand how to classify threats,
- Perform vulnerability identification and classification based on the organization's profile,
- Perform a control analysis for a selected organization,
- Understand how to perform a likelihood determination using both quantitative and qualitative methods,
- Be able to conduct an impact analysis, based on business and management requirements,
- Use the knowledge of processes land above in order to complete a risk determination for an organization,
- Identify control recommendations for the organization and understand the various types of control and implementation programs that are available,
- Developing the skills to enable the auditor to effectively document the results of the above processes,
- Identify pertinent standards and regulations and their relevance to information security management,
- Describe legal and public relations implications of security and privacy issues.

As such, completion of the program should develop the knowledge within its people necessary to allow it to:

- Identify critical information assets within an organization that they are familiar with,
- Identify and specify security controls for a variety of systems,
- Specify effective monitoring controls and understand how these may be implemented within an organization.

Risk Assessment

In today's environment of severely constrained resources (both staffing and financial) investments in security controls must show a positive return on investment. Information security can be viewed as an enabling investment, reducing operational costs or opening new revenue streams, or as a protective investment, preventing potential costs or negative business impacts. In either case, the cost of the security controls must be appropriate for the risk and reward faced.

In simple terms, a risk is realized when a threat takes advantage of a vulnerability to cause harm to your system. Security policy provides the basis for implementing security controls to reduce vulnerabilities thereby reducing risk. In order to develop cost effective security policy for protecting Internet connections some level of risk assessment must be performed to determine the required rigor of the policy, which will drive the cost of the security controls deployed to meet the requirements of the security policy. How rigorous this effort must be is a factor of:

- The level of threat an organization faces and the visibility of the organization to the outside world
- The sensitivity of the organization to the consequences of potential security incidents
- Legal and regulatory issues that may dictate formal levels of risk analysis and may mandate security controls for specific systems, applications or data.

Note that this does not address the value of information or the cost of security incidents. In the past, such cost estimation has been required as a part of formal risk analyses in an attempt to support measurements of the Return on Investment (ROI) of security expenditures. As dependence on public networks by businesses and government agencies has become more widespread, the intangible costs of security incidents equal or outweigh the measurable costs. Information security management time can be more effectively spent assuring the deployment of "good enough security" rather than attempting to calculate the cost of anything less than perfect security.

For organizations that are subject to regulatory oversight, or that handle life-critical information, more formal methods of risk assessment may be appropriate. The following sections provide a methodology for rapidly developing a risk profile.

It can be prohibitively expensive and probably impossible to safeguard information against all threats. Therefore, modern Information Security practice is based on assessing threats and vulnerabilities and selecting appropriate, cost-effective safeguards. A realistic approach is to manage the risk that these threats pose to information and assets.

It is recognized industry best practice for all organizations to identify their information assets and apply the appropriate security measures based on a Threat and Risk Assessment.

To help organizations meet this requirement, many organizations use industry standard methodologies which have been developed to assess the value of the information that the organization is processing and allows greater flexibility for providing recommended safeguards.

The assessment process

The following diagram illustrates the four-phased approach to performing a Threat and Risk Assessment.

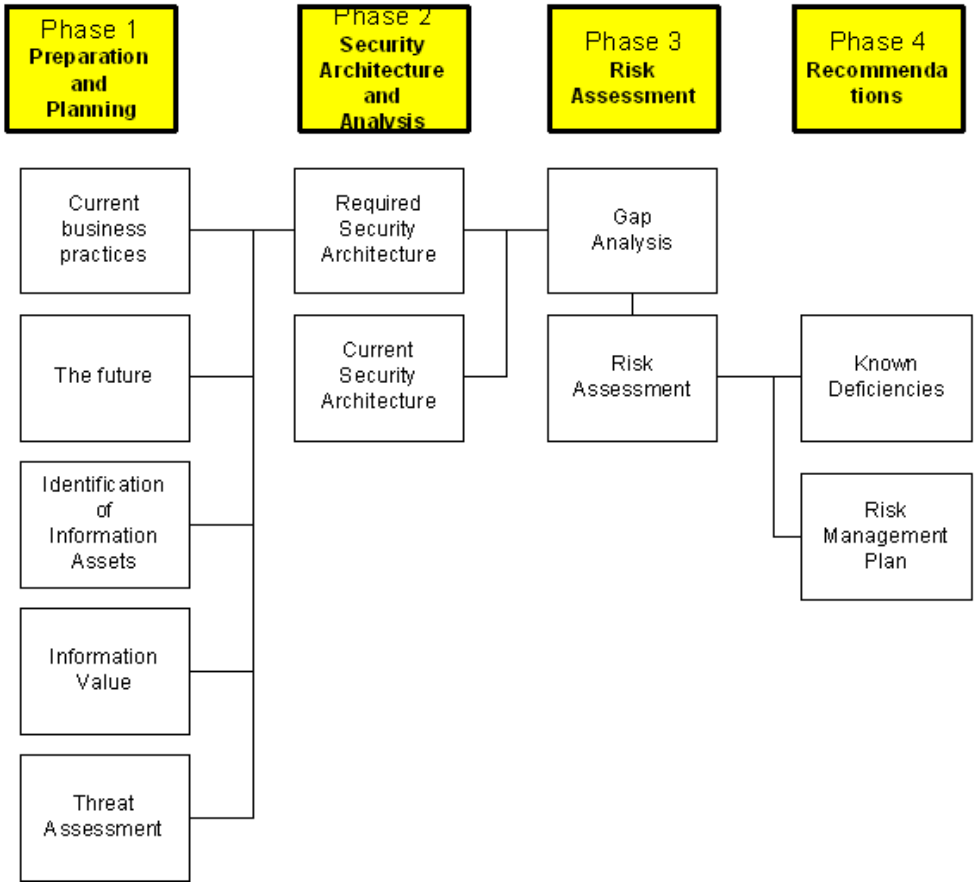

Figure 26-1 Risk Assessment Methodology

Phase 1 - Preparation and Identification

Current Business Practices

The first step in performing a Threat and Risk Assessment is to define the business practices that are required by the organization to accomplish corporate goals. The Current Business Practices of the organization are documented by analyzing the organization's mission statement, corporate plan, type of clients and the services that it provides.

The Future

It is critical that the organization's future business practices and corporate goals are considered throughout the Threat and Risk Assessment process. The future plans of the organization must be documented at the start to avoid any possible oversight, preventing the assessment being dated within a short period of time.

Identification of Information Assets

The organization's information assets are identified to determine what has to be protected. This requires producing an inventory that lists all information systems and their assets. Each list typically includes the following information:

- the system owner,

- the system's location,
- the nature of business,
- the type of information processed,
- the purpose or application of the system,
- the system configuration,
- the user community, and
- any known inherent strengths or weaknesses of the system.

Information Value

After an inventory of the information assets has been produced a Statement of Sensitivity is documented for each asset. This documents the asset's importance and value to the organization and should reflect its criticality. The statement is produced by analyzing the system and the data it processes with regard to integrity, confidentially and availability requirements.

Threat Assessment

The next step is to identify all threats and threat sources to the organization's information assets and assign a classification that reflects the probability of it occurring. The five levels of threat classification are defined as follows:

- Low: There is no past history and the threat is unlikely to occur.
- Low Plus: There is no past history and the threat could occur.
- Medium: There is some past history and the threat could occur.
- Medium Plus: There is some past history and the threat is likely to occur.
- High: There is significant past history and the threat is likely to occur.

Phase 2 - Security Architecture Analysis

Required Security Architecture

The information gathered in phase I is used to document the business requirements for security within the organization. The key security strategies are identified that will enable the organization to effectively protect its information assets.

Each pre-determined threat to the information assets is matched with an effective safeguard or safeguards. A safeguard is described as a number of Security Enforcing Functions (SEFs) and associated mechanisms that perform that function are the Security Mechanisms (SM). The process of identifying the required SEFs and the associated mechanisms gives the Organization a security architecture baseline to work towards.

Identification of Current Security Architecture

The organization's current security architecture is documented to identify existing Security Enforcing Functions (SEF) and Security Mechanisms (SM). These safeguards and any existing policy or doctrine are identified so as to produce the current security baseline. This enables identification of differences between the current and required security baselines.

Phase 3 - Risk Assessment

Gap Analysis

A gap analysis is performed to highlight any differences between the organization's current security architecture and the required security architecture, determined in phase II of the assessment. The output from this analysis will give the reviewer an indication of the residual risk.

Risk Assessment

After the gap analysis has been performed the determined residual risk has to be assessed. This assessment produces a level of risk that is measured by the probability of compromise to the confidentiality, integrity or availability of the designated information system and the data processed on it. Determining the level of risk is completed by comparing the relationship between the threats associated to the residual risks and known vulnerabilities or weaknesses.

Phase 4 - Recommendations

Known Deficiencies

Where the assessment of the systems safeguards indicates that they are not able to effectively counter known threats, additional safeguards will be recommended so as to reduce the risk to an acceptable level. The reviewer will also recommend the type of safeguard required its priority and suggested schedule of implementation.

Risk Management Plan

The Threat and Risk Assessment process provides the system manager with an appreciation of the status of the safeguards protecting information assets within his/her organization. An assessment of the adequacy of existing safeguards is performed so as to provide recommendations to assist the system manager in making an informed decision as to which risks the organization should manage or accept.

The level of acceptable risk is a managerial decision that should be based on the information and recommendations provided in the Threat and Risk Assessment.

Assessment and Conclusion

This methodology has been successful in providing assessments for organizations by producing relevant results. This is achieved by considering the business value of information and the business practices of the organization.

The four-phased approach provides a logical progression, which enables the client to trace through the results from each phase to see how the recommendations were obtained.

Risk Management

Most Security Professionals typically recommend and use a four-phase approach to implementing a comprehensive, enterprise-wide security management program:

Risk Management is an Issue for Management, not Technology

The first phase identifies the critical information assets in order to understand the nature and severity of security risks and exposures to those assets. Types of exposures include:

Confidentiality -- the exposure if information gets into the wrong hands
Integrity -- the exposure if the wrong information is used to make decisions
Availability -- the exposure if information is not available for use when needed.

This "Business Value Assessment" identifies owners for critical information assets, evaluates security classification levels, and documents the usage and residence of critical information. The deliverable, an Information Asset Profile, provides a "control book" that highlights which information requires protection, what kind of security is important for the business use of that information, who has ownership responsibility, and how and where the information is primarily used. This enables an information security program to be tailored in the next three phases to provide the right types of controls and mechanisms for the most critical information to the business.

The second phase determines how information assets should be protected. In this phase, the management philosophy and results of the Business Value Assessment are used as guides in defining the guiding security principles for the organization. Where needed, existing security policies and standards are updated and new ones are developed. In conjunction with a standard of best practices for security management (ISO17799/27001), all relevant aspects are addressed to produce a customized security architecture that effectively aligns to strategic IT and business needs.

When the third phase can use your organizations specific security architecture as a model, you map current processes to the defined security processes in your organizations security architecture and identify gaps. International Standard ISO1799 is often used as the model in lieu of one provided by many security consultants. Security assessment activities should include a comprehensive review of an organization’s policies, procedures, and information protection mechanisms. Recommendations are developed that specify actions to close the gaps with an implementation strategy based on your organization’s unique business needs.

In the final phase, recommendations are implemented. Implementation requires overall project and transition management, evaluating and recommending products and tools, conducting employee awareness training, or assisting with migrations and conversions. Properly implemented process feedback mechanisms will ensure continuous improvement in security management quality.

Security should be commensurate with risks .The process to determine which security controls are appropriate and cost effective, is quite often a complex and usually subjective. The prime function of security risk analysis is to put this process onto a more objective basis.

As stated above, there are a number of distinct approaches to risk analysis. These may be defined in two types: quantitative and qualitative.

Constraints Analysis

When starting a risk program, examine requirements outside of your control:

- National, international laws on topics such as pornography, privacy of employee and customer data, libel etc. should be taken into account.
- Corporate requirements (mission, strategy etc.).
- Budget (unless money is no object!).

Risk summary

Once the threats, impacts and corresponding risks have been listed and the constraints have been analyzed, the significant business risks (or weaknesses) will be more evident, allowing a counter strategy to be developed.

It is advisable to summarize the risks to be countered together in one table. Likewise a summary of major strengths would show what has been achieved to date. An example of the major risks/weaknesses list might be:

- Management does little to encourage and support security measures.
- There is an inadequate information security policy, information is not classified.
- Users are not security aware and generally use bad passwords. Unused terminals are rarely protected.
- Few computers are installed with homogenous, standard software. Most users install what they want on their machines.
- The Internet connection to the company is made by a weak Firewall, with few access control mechanisms, no audit log, no official policy and no monitoring/intrusion detection or incident response team.
- Certain servers are not kept in locked computer rooms, have no backup power circuit, air-conditioning or static/electromagnetic protection.
- Few computer operating procedures are documented.
- No off site tape backups are made.
- Employees are not identified adequately, visitors may roam unchecked (no visitor procedures, lack of building security).
- The building is in an earthquake zone, where minor quakes are expected every 30 years.
- The network control room is underground and may be subject to flooding during major storms.

Counter strategy & counter measures

Develop a strategy, based on the Risk Summary above to:

- *eliminate* risk, or
- *reduce* the risk to an acceptable level, or
- to *limit* the damage (reduce the impact of a threat), or
- to *compensate* the damage (insurance).

Countermeasures typically involve: Security Policy, Security organization (responsibility, roles & processes) and specific mechanisms.

1. Definition of security policies, to protect information based on the risk (see the "Policies" chapter). Policies *reduce* risk.
    - Definition of a corporate security policy.
    - Definition of policies on a project, system or business unit basis.
    - Distribution of policies to those affected.
2. Implementing Policies: Roles, Responsibility and organization are required (see next chapter). A security organization can *reduce* risk and *limit* damage.
    - The IT security organization needs a clear statement of mission and strategy.
    - Definition of security roles & processes.
    - Users, administrators and managers should have clearly defined roles/responsibilities and aware of them.
    - User / support staff may require training to be able to assume the responsibilities assigned to them.
3. Define requirements on mechanisms: Effective use of mechanisms and processes to enforce security. Choosing appropriate security mechanisms together with secure operating procedures can *reduce* the risk. Requirements should be listed under the following (ITSEC recommended) headings. ITSEC also recommends that the *strength* of mechanisms and countermeasures should be rated as *basic*, *medium* or *high*.
    - Identification and Authentication
    - Accountability
    - Audit

- Access Control
- Object Reuse
- Accuracy
- Data Exchange
- Reliability of Service

4. Define concrete Secure Operating Guidelines and controls for specific systems (see Part III).
5. Consider insuring against threats which cannot be covered by the above measures.
6. Assurance / constant vigilance:
    - Conduct regular audits of important systems. How effective are the countermeasures, do they require tuning?
    - Reconsider risks regularly. Are new threats more important, have some threats ceased? Risk and strategy should be reconsidered regularly (perhaps once every year or two).

Business Impact Analysis

A business impact assessment (BIA) involves the creation of formal documentation that details the impact various disruptions would have on the organization. The details of this documentation consist of potential financial or quantitative loss, potential operational or qualitative loss, and vulnerability assessment.

The three primary goals of any business impact assessment are:

1. **Criticality prioritization** – identifies and prioritizes each and all critical business/operations unit process, and evaluates the impact of a disruptive event or incident.
2. **Downtime estimation** – an approximation of the greatest acceptable downtime that the business or operation can endure while still remaining viable (i.e., what is the longest time a critical process can continue to be unavailable before the organization can never recuperate?).
3. **Resource requirements** – this phase involves the analysis and documentation of the resource requirements required for the organizations critical processes. It makes certain that the most resources are allocated to time-sensitive processes.

A business impact assessment has four steps:

1. gathering the needed assessment materials
2. performing the vulnerability assessment
3. analyzing the information compiled

4. documenting the results and presenting recommendations

Defense in Depth

DISA, (Defense Information Systems Agency) has one of the best definitions for Defense in Depth:

"*The Defense in Depth approach builds mutually supporting layers of defense to reduce vulnerabilities and to assist us to protect against, detect, and react to as many attacks as possible. By constructing mutually supporting layers of defense, we sill cause an adversary who penetrates or breaks down one defensive layer to promptly encounter another, and another, until unsuccessful in the quest for unauthorized entrance, the attack ends. To protect against different attack methods, we must employ corresponding security measures. The weakness of one security measure should be compensated for by the strength of another."*

When reviewing an organizations risk, always consider the impact of a control failure. If one system or control fails, what happens to the rest?

"Defense in Depth: Foundations for Secure and Resilient IT Enterprises" by Christopher J. May, Josh Hammerstein, Jeff Mattson and Kristopher Rush (September 2006) is available freely from CERT as CMU/SEI-2006-HB-003. This document is one of the best programs for anyone wishing to know about defense in depth – in depth.

Data Classification

Data Classification is the conscious choice to allocate a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of any intellectual property should be determined by the extent to which the data needs to be controlled and secured and is also based on its value in terms of worth as a business asset.

The classification of all IP (including data and documents) is indispensable if an organization is to differentiate between that which is a little (if any) value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. Systems may then be used to catch keywords and terms used in the classification.

Conclusion

Information Systems Risk Management is a complex topic. These processes have been developed to enable auditors with different levels of Information Systems security experience and indeterminate quantitative mathematical knowledge to be able to understand Information Systems risk in a manner that they can use immediately.