



Security by Design

ENTERPRISE RISK ASSESSMENT OVERVIEW

March 2005 version 1.0

Nicholas Vennaro

Issue Overview:

Companies are spending significant sums of money on information security. However, most business and technical leaders report that they are securing the wrong assets or are not sure how effective their security strategy is at safeguarding their critical resources. A formal and systematic risk assessment is a critical first step to any enterprise security strategy.

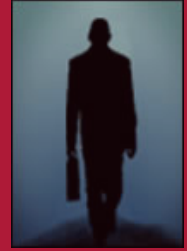


Table of Contents

| | |
|---|----|
| Summary..... | 3 |
| Enterprise Risk Management..... | 3 |
| Understanding and Defining Risk..... | 4 |
| Critical Component - Risk Assessment..... | 5 |
| Risk Assessment Methodologies | 6 |
| OCTAVE..... | 6 |
| CRAMM..... | 8 |
| Scenario Based | 8 |
| Limitations of Risk Assessment | 9 |
| Tools are the solution | 9 |
| Comfort with status quo..... | 9 |
| Lack of documentation | 10 |
| Focus on outside threats | 10 |
| Critical Success Factors | 10 |
| Senior management sponsorship..... | 10 |
| Documented process | 10 |
| Business unit involvement..... | 11 |
| Integration into major processes | 11 |
| Closing..... | 11 |

Summary

Enterprise Risk Management (ERM) is first and foremost a business issue, not a technical prerequisite. An enterprise risk management process is put into place and implemented because it is part of the organization's business objectives. ERM should be undertaken within the context of the overall business mission of the organization.

With that said it is a complex set of trade-offs that have to be understood to protect a company's key assets from the most harmful threats in the environment. Determining what the critical assets are and the corresponding threats against them is the risk assessment phase of ERM. Risk assessment is the key component of the entire enterprise risk management process and will provide the framework for the entire effort.

Assessment methodologies exist that help to insure the most critical assets are protected and therefore that security dollars are spent wisely. By utilizing one of these methodologies business leaders and technologists within companies can begin to deploy the proper tools and procedures to safeguard vital corporate assets. The pros and cons of the most common methodologies are described in this report as well as some of the limitations of ERM and risk assessments.

Enterprise Risk Management

Large sums of money are being wasted on the wrong security efforts inside most companies. This is caused by a number of factors:

- *Not sure what to secure* – If you don't have an understanding of the critical assets in the environment then you can not be executing on a coherent strategy of securing your most important resources. In an environment such as this, leaders tend to overspend in a shotgun approach to security.
- *Don't understand the threats* – This follows from the first point above. Assets can have quite different threat profiles but if you are unsure of the critical assets then building an accurate threat profile is impossible.
- *Tools are easy to buy* – Vendors are all too happy to sell tools and it becomes tempting to buy a tool, role it out and then declare victory. While this makes everyone feel good security is not enhanced.
- *Limited business involvement* – all too often security projects are spawned by perceived technical threats out of context with the business drivers in the environment. I have been in numerous organizations where the reason for implementing a particular project was "the security group said we had to..." For a risk management program to be effective it has to become part and parcel to the business mission of the organization.

An enterprise risk management strategy is the process of putting a set of systematic controls and processes into place that will reduce uncertainty, manage the threats in

the environment, and provide a level of comfort in knowing that the critical components in the environment are protected to a reasonable level given the business goals and mission of the enterprise. The process then requires that the enterprise monitor, evaluate and fine tune the controls that have been put into place. Lastly, companies must look for ways to promote security awareness across the enterprise, making security a company initiative not the purview of one department.

Companies tolerate various levels of risk. This risk tolerance is based on a number of complex and interrelated factors such as: organizational culture, business domain, government regulatory policies, and international political issues. Each company will need to weigh and decide these factors individually. However, no matter where you find yourself on the risk tolerance scale, there are four general responses to risk:

1. *Acceptance* – you may find it appropriate to accept the fact that there is a risk and if there is a loss it will be absorbed.
2. *Transference* – in this case the risk is assigned to a 3rd party; an insurance company for example. If there is a loss the 3rd party will absorb all or part of the loss for you.
3. *Mitigation* – through a set of controls or processes the risk is reduced to some acceptable levels.
4. *Avoidance* – the risk is avoided in most cases by abandoning some business arrangement. This may be terminating a business accord with a 3rd party or not creating a particular product.

The first step in creating an Enterprise Risk Management solution is to understand your critical assets, threats and risks against those assets then a program to respond to the risks can be adequately developed. This is the *risk assessment* phase in ERM and the main focus of this paper.

Understanding and Defining Risk

Typically, inside major corporations the term risk has various meanings. An auditor, a CEO, and an actuary will all have different opinions as to the definition of risk and how it affects the organization. It is important then to define a few terms as they related to information security and risk:

- *Risk* – a risk in the environment is the likelihood that a given threat will exploit a specific vulnerability in a system or process.
- *Threat* – any event that causes an undesirable consequence to an organization.
- *Vulnerability* – a weakness in a safeguard that is protecting an asset.
- *Asset* – something – resource, equipment, process or product – that the leaders in the organization decide needs protecting.

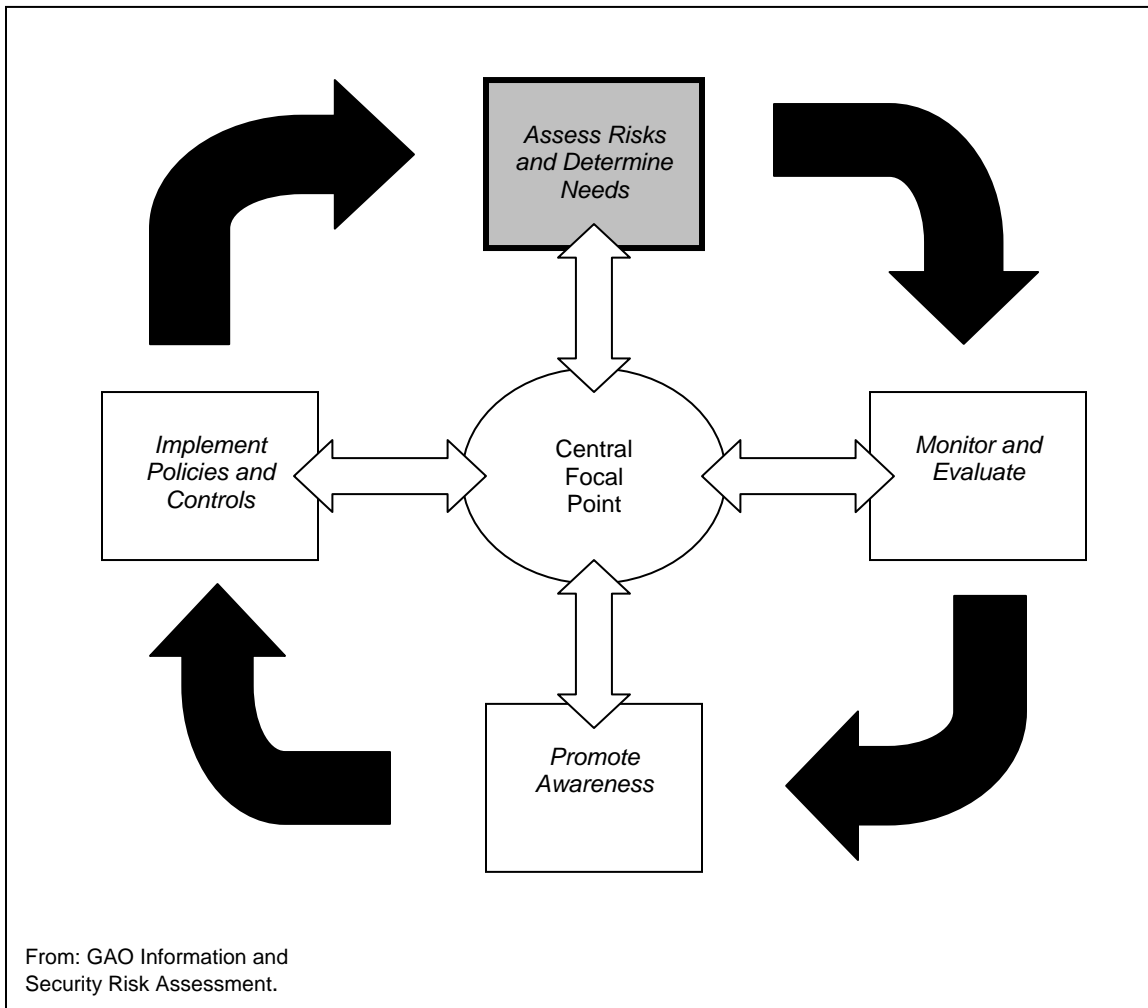
Taken together; assets, threats, and vulnerabilities are called a triple in the information protection domain.

Ultimately, the goal for risk assessments is to understand the risks in the environment and develop a strategy to mitigate them until they are at an acceptable level. The goal is not to eliminate risk all together; that would be counterproductive.

Think of a company that is trying to eliminate bad debt. Taken alone, bad debt does not sound like a good thing to have; we all want our customers to pay their bills. However, the company that has zero bad debts has more than likely missed sales opportunities. The goal with bad debt is to keep it to some low level 2% of sales for example because the cost of eliminating it (lost sales) is higher than the benefit. The same holds true for risk mitigation.

Critical Component - Risk Assessment

The General Accounting Office defines the risk management cycle as illustrated below:



The critical nature of risk assessments in leading organizations is stressed in the General Accounting Office (GAO) report *Information Security Risk Assessment*. "Risk assessment is an essential element of risk management." The report goes on to state: "**Although all elements of the risk management cycle are important,**

risk assessments provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selection of cost-effective techniques to implement these policies.”¹ (Emphasis added).

The importance of risk assessments in the entire process is borne out by my work with Fortune 1000 companies across the United States. The risk assessment process provides the foundation for all components of the enterprise risk management process that come after it.

The fact that risk assessments are a critical underpinning to the entire Enterprise Risk Management strategy it follows then that the assessment methodology you choose is crucial to the success of your security effort.

Risk Assessment Methodologies

There are two broad categories of risk assessment methodologies; quantitative and qualitative. These categories are not necessarily mutually exclusive; companies can use different methods at different times depending on needs.

The major difference between the two categories is straightforward. The *quantitative* method attempts to assign independently developed numeric values to components of the risk assessment. For example, dollar cost of an asset or loss due to a realized threat. The *qualitative* method on the other hand is more subjective in nature and focus on the more intangible aspects of a loss.

A quantitative approach usually makes people feel more comfortable with their decisions. Complex calculations are performed to derive items such as Exposure Factor, Single Loss Expectancy, Annualized Rate of Occurrence, and Annualized Loss Expectancy. This may be providing a false sense of security because the estimates used to calculate this information can vary widely. Case studies that have been conducted have found that companies that used simple tools and a qualitative measure were the most cost effective and usually the most successful.^{2 3} It is important to note that risk assessments are not one and done. That is; they are iterative by design, so you can adjust your qualitative approach with each iteration in the process.

No matter which method of security risk assessment that is used the steps are typically the same – Identify the asset, determine risk(s), calculate likelihood of occurrence, and develop a strategy to mitigate or accept the risk.

OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk assessment methodology that uses qualitative measures to analyze IT risk. This

¹ *Information Security Risk Assessment*, GAO November 2000.

² *Burton Group Risk Management Concepts and Frameworks* July 2004.

³ *GAO Information Security Risk Assessment* November 2000.

methodology was created by the Software Engineering Institute (SEI) at Carnegie Mellon University. It has broad support in government agencies and its adoption in the private sector is on the rise.

The notion of self-direction is integral to the OCTAVE approach. Information security is the responsibility of everyone within an organization and as such it is the responsibility of a broad cross section of people to direct and manage the security process for the enterprise. While this is good in principle in practice it tends to be the people in the IT area that are driving the security initiatives. However the more security becomes part of the normal business process the more reliable the controls will be and the enterprise will be more secure for it.

The OCTAVE process tends to focus on the operational aspects and systems across the organization and how these operational systems are vulnerable to threats in the environment. During the OCTAVE process a cross functional team is assigned to the project to determine critical assets of the organization, develop threat profiles/vulnerabilities, decompose the assets into their components, and ultimately to develop a protection strategy.

OCTAVE Phases

The OCTAVE methodology is broken down into eight processes across three phases.

Phase 1: Organizational View (Process 1-4) – It is in this phase that a set of questions are posed to individuals across the enterprise to get various points of view on critical assets and threats in the environment. This knowledge survey process falls into three perspectives; Senior Manager, Operations, and general staff. It is in this phase that the critical assets of the organization are determined.

Phase 2: Technological View (Process 5-6) – It is in this phase that critical components of the infrastructure are evaluated. As the critical assets are identified the components that the critical assets depend upon are evaluated for technology vulnerabilities.

Phase 3: Risk Analysis (Process 7-8) – It is in the final phase that the OCTAVE team identifies the risks to critical asset components and develops a protection strategy/mitigation plan to safeguard the assets.

OCTAVE in Practice

OCTAVE is a fast, flexible and efficient methodology for capturing key assets in the organization and preparing a risk mitigation strategy around those assets. The strength of OCTAVE – the usage of a cross functional team with strong interdisciplinary skills to accurately understand the enterprise issues, is inherently difficult to implement if the organization lacks commitment to the process. Resources do not have to be dedicated for a long period of time; but while the process is taking place they have to be committed to the effort.

There has been criticism that OCTAVE is too “heavy” and paper intensive. Like any methodology the good practitioner takes what is needed to solve the problem at hand. OCTAVE as designed by the SEI is paper intensive. The authors of the methodology have gone to great lengths to document job aids, process maps, training materials, and document the steps necessary to run an effective risk

analysis session. To alleviate the paperwork burden AegisSecurityWorks has automated the OCTAVE process, see www.AegisSecurityWorks.com.

The OCTAVE methodology has been readily adopted by government agencies such as NASA and the DOD. Its acceptance by the private sector is rising steadily, this may be due in part to fact that the methodology is freely available, it's easy to implement, and federal acceptance and utilization provides a level of comfort.

CRAMM

CRAMM, the Risk Analysis and Management Method was created and administered by the department of Security Services of the United Kingdom. CRAMM is a facilitated risk analysis method that attempts to discover critical assets and vulnerabilities by presenting a series of questions to participants.

The results of the questions are entered into a hierarchical dB for analysis and reporting. CRAMM is very useful in determining interdependencies between assets and business systems that they are related to. The CRAMM methodology is also very robust for the asset and threat identification process. The tools and process documentation is very thorough for this area. For example, tangible and intangible assets are fully considered as is the threats to those assets and the likelihood that those threats will materialize.

CRAMM in Practice

CRAMM has broad functionality in that it can be implemented for a wide range of uses – systems development, compliance/audit, and disaster/continuity planning. The fact that CRAMM is tool based as well as a methodology has made its adoption easier than OCTAVE.

CRAMM is widely accepted in the UK and other western European countries but adoption is very sparse in the United States. CRAMM appeals to organizations who favor a quantitative approach as it has qualitative as well as a quantitative components within the methodology. The tools that are available for CRAMM facilitate “what if...” scenario creation, allowing the practitioner to study various tradeoffs in the risk analysis situation.

Scenario Based

This technique involves the creation of various scenarios that depict how a computer system can be compromised. Threat scenarios get created by organization subject matter experts and countermeasures are then proposed, tested, and implemented.

The scenario based approach requires brainstorming sessions with internal and external experts from within the company. This is a relatively inexpensive way to test out numerous threat situations and “think out loud” about potential threats to assets in the enterprise. When this technique is employed it is very interesting to observe the ways in which the conversation develops as the team begins to think of novel ways the enterprise could be compromised. The scenario based approach is very flexible in that the team can switch focus between situations quickly – analyzing

employee threats, outside threats, computer malfunctions, and network attacks, etc all very easily.

Scenario Based in Practice

This technique while flexible it is difficult to analyze the interrelationships between and across threat scenarios. Humans are very good at switching context and thinking of new and creative methods to “attack” their enterprise (to expose vulnerabilities). Humans (without tools) are not good at keeping track of all the interrelationships of those scenarios. At present, there is not a good tool on the market place to track the scenarios or perform “what if...” analysis on various threat scenarios.

The focus with Scenario Based risk methodology is generally on threat scenarios; rarely is a detailed analysis done to determine critical enterprise assets. This lack of asset analysis can lead to the wrong assets being protected. It has been my experience that scenario based risk assessment works best when done in conjunction with another methodology. For example, OCTAVE can be used as the primary risk assessment method and after assets where identified the team could create risk scenarios against those critical assets. This has the effect of focusing the scenarios.

Limitations of Risk Assessment

There are a number of common misunderstandings and limitations to the risk assessment process. Many of the limitations and false assumptions are part of everyday life and the security processes and methodologies are not immune to this.

Tools are the solution

It is very common for clients to become very complacent after a tool is purchased. I am reminded of a colleague who was fond of saying “A fool with a tool is still a fool...” There is always significant pressure to pick a tool to fix the problem at hand. When in most cases what is needed is some level of analysis of the issues, assigning the right subject matter experts, and most of all realize that ERM is not a one time event – it’s long-term, it’s iterative, and it’s constantly changing.

This of course is not to say that tools are not necessary but they are not sufficient to solve the enterprise risk management problem.

Comfort with status quo

As time passes and nothing bad happens the tendency is to let your guard down. Typically, procrastination follows – controls are put off, expenses are cut, or teams are pulled to work on other projects.

The more you have weaved security into the fabric of your organization the easier it is to guard against this problem. If information protection and security becomes part of every project and part of everyone’s job then this comfort level is less likely to seep into the organization.

Lack of documentation

The rationale for decisions or even the decisions themselves can be lost if documentation is not written and saved. As the ERM process moves forward it is critical that the decisions from one session to the next are saved, critical assumptions are documented, and thought leaders insights are captured. This will facilitate the iteration of the next phase as well as providing the back up necessary in case of a failure to reconstruct the problems and prevent them in the future.

Focus on outside threats

In general, companies tend to focus too much time and resources on outside threats and not enough on internal threats from business partners and employees. From an information protection standpoint there is usually more to fear from a disgruntled employee or a clerk selling social security numbers for \$25.00 a piece than from outside threats.

This is an example of how the popular press influences our perceptions. It is the large security breaches that get the attention but you most likely have more to fear from your own employee and those incidents are not in the news papers. Here is where scenario based risk management can help. Employees are very likely to pick up on weak internal controls and note where a system can be spoofed.

Critical Success Factors

Senior management sponsorship

The single most important determinant of a successful enterprise risk management strategy/implementation is the involvement and support of senior management. Without senior management support for the effort the process will flounder as resources are pulled for other efforts.

Senior management involvement comprises – verbal support for the effort, assignment of resources, involvement in developing the process and determination of scope and ultimately support for the recommendations that flow from the process.

Documented process

Enterprises that choose an industry standard methodology and document the process will find that the chance of a successful implementation increases dramatically. The use of a standard methodology will allow outside resources to be added to the effort as needed and increase the options for training of staff members.

A documented process allows a more detailed analysis to take place, facilitates data sharing, and aids in an iterative procedure. Defining clear communication channels and other good project management controls will of course help to create a successful Enterprise Risk Management strategy effort.

Business unit involvement

This paper started with the statement that Enterprise Risk Management is a business not a technical matter. Not surprisingly then one of the key success factors is involvement of the business resources in the process. ERM and more specifically risk assessment to be successful must be part of the overall business objectives.

As risk management is integrated into the business process the subsequent strategy sessions and information protection in general will become second nature and part of the business areas "day job" not an effort that happens once a year when the technical group mandates it.

How best to facilitate business involvement? It starts with senior manager commitment (see above) and understanding of the process. Involving key individuals early in the process increases dedication to the effort. Explaining technical aspects to the business community and business nuances to the technical staff will assist in bridging the gap between both constituents. Most of all, if you function like a team, camaraderie and understanding will develop.

Integration into major processes

Integrating Enterprise Risk Management procedures into the processes within the organization will go a long way in institutionalizing the effort and increasing the chance of successful implementation.

The organization processes that risk management should be integrated with is the software development life cycle (SDLC), project management office (PMO) procedures, quality assurance (QA) gates and methods, disaster continuity plans, and business strategy efforts.

The more security in general is integrated with the processes and procedures of the organization the more likely the risk assessment effort will be successful

Closing

Risk assessment – determining the key assets within the organization, analyzing the threats against those assets so an effective risk mitigation strategy can be developed -- is the cornerstone of Enterprise Risk Management.

To efficiently and effectively assess risk in an organization an industry standard methodology, such as OCTAVE or CRAMM should be employed. A documented methodology will dramatically increase the organization's chances of success.

There are critical success factors that can be employed during the risk management and assessment project that will increase the chances of success – involve the business units and senior management, document your assessment process, and integrate the risk assessment procedures into the organization's processes and procedures whenever and wherever possible.