Global Information Assurance Certification Paper

An Introduction to Information Risk Assessment

Vishal Visintine

GSEC Practical, Version 1.4b

August 8, 2003

1. Abstract

An understanding of risk and the application of risk assessment methodology is essential to being able to efficiently and effectively create a secure computing environment. Unfortunately, this is still a challenging area for information professionals due to the rate of change in technology, the relatively recent advent and explosive growth of the Internet, and perhaps the prevalence of the attitude (or reality) that assessing risk and identifying return on investment is simply too hard to do. This has kept information systems and information systems security in the undesirable position of being unable to systematically identify and monetarily quantify security risks. This in turn has led to inconsistent and inappropriate applications of security solutions as well as either excessive or insufficient funding for such activities. Therefore this paper addresses the issue of risk with respect to modern information systems and seeks to answer the following questions:

- What is risk with respect to information systems?
- What are the key elements of information security risk?
- Why is an understanding of risk important?
- What are the key elements of a risk assessment?
- What are some of the common risk assessment methodologies?

2. Risk Defined

> Risk – "The possibility of suffering harm or loss; danger." [1]
>
> "Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity." [2]

What is risk with respect to information systems? Risk is a measure of the impact of something undesirable happening and its likelihood of occurring ideally expressed in dollars and frequency. This can be applied to almost anything. For instance, it can be in reference to the risk of an earthquake occurring, taking a loss on an investment such as stocks (as many people have in recent years), or someone hacking into a database containing sensitive information such as financial records. Risk, at its most fundamental, is an acknowledgement of the fact that life is uncertain and that there are variables both within and outside of our control and awareness that can play a major role in determining the outcomes of things both small and large. Risk, in a more practical sense, is our attempt to measure and compensate for known and unknown factors that affect our ability to achieve goals. There are two primary ways that risks are measured: quantitatively and qualitatively.

2.1. Quantitative Risk

Quantitative risk is the process of measuring risk in terms of money and frequency. When risk is measured this way, one can compare the costs of risks against the costs of implementing security solutions to reduce or eliminate those risks. In business, this

[1] Query for "risk". Dictionary.com
[2] Van Scoy, Roger L. *Software Development Risk: Opportunity, Not Problem*

would be called return on investment analysis (ROI) which is a common way to justify taking a certain action or justifying why not take it. Mathematically, quantitative risk can be expressed as Annualized Loss Expectancy (ALE) which can be determined according to the following formula:

ALE = Asset Value x Exposure Factor x Frequency (annual rate of occurrence)

The **asset value** is, as the name suggests, the total value of an asset. The **exposure factor** is the percentage of the asset's value that is exposed. For example, an insurance business may have a very large cash reserve that is exposed to losses to due claims and law suits. This is of course one of the purposes of having cash in reserve for an insurance company. But, if the total claims (legal or otherwise) cannot exceed 50% of the cash reserve then it has only has a 50% exposure for that asset. The **frequency** is the measure of how many times a loss will be incurred over an average year. If, on average, a claim is only made every two years, then the frequency is 0.5. If it occurs ten times a year, then it would be 10. These three factors combine to produce the ALE which is essentially the monetary risk for a given asset with respect to certain exposures or threats. When all assets and exposures have been identified and factored together, an overall assessment of the monetary risk can be obtained.
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. [1]

2.2. Qualitative Risk

Qualitative risk assessments seek to identify and rate risks relative to each other. In contrast to quantitative risk, the perceived impact of the loss, corruption, or unavailability of an asset is determined. The key elements of qualitative risk are: Asset Value, Vulnerability, Threat and Controls. Note that the exposure factor is not present and nor is the frequency of occurrence. This information is not assumed to be available, so instead vulnerabilities and threats are identified. These values help to establish which risks are greater than others. Controls will be discussed later.

As an example, let's say someone wanted to gather and keep their money safe by leaving it on the ground in a public area of a major city. Obviously, this isn't a good idea, but it is risky so we can work with it. This very simple example contains three of previously mentioned elements of risk, namely: assets, vulnerabilities, and threats.

2.2.1. Assets

As with quantitative risk, an **asset** is anything of value. In this case, the monetary value may not be clear but its relative value (with respect to other assets) is. This could be

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

money, as in this example, it could be a server, it could be data, or could be a company's reputation. In terms of risk, assets are what we want to protect.

2.2.2. Vulnerabilities

A **vulnerability** is anything that could be exploited to gain or deny access to an asset or otherwise compromise an asset. Vulnerabilities are generally a lack of protection or the exploitation of something that can be used to gain access to an asset. In the example above, the money would be highly vulnerable because it is completely unprotected. If **controls**, means of protection, were put into place the vulnerability would be reduced. Controls are not part of the above risk formula, but they are factored in because vulnerabilities and controls are really different ways of looking at the same thing. When there are strong controls, vulnerabilities are few. When there are large vulnerabilities, there are few strong controls (generally speaking). Vulnerabilities are also sometimes expressions of controls – a control may reduce or eliminate one vulnerability but create another. For example, an armed guard might be a powerful to deterrent to most bank robbers. However, an unarmed robber who is able to overcome the armed guard can take his or her gun and will thus have more power than he or she had before. In this second case, the introduction of the armed guard (the control) reduced one risk but created another.

2.2.3. Threats

A **threat** is anyone or anything that can exploit a vulnerability to obtain, alter, or deny access to an asset. Examples of threats include hackers, tornados, poor procedures, lightning, human error, terrorists, etc. Threats exist with respect to vulnerabilities and there can be multiples threats for each vulnerability. Furthermore, threats are sometimes broken into categories such as human/non-human, intentional/unintentional, skilled/unskilled, and internal/external. These distinctions can help in determining which threats are the most dangerous and thus focus activity on controls that will reduce their potential impact. A virus, for instance, is non-human, intentional (it was designed with a purpose), could be skilled or unskilled depending on the developer of the virus, and are generally (at least initially) external threats. On the other hand, a disgruntled systems administrator is human, intentional, skilled, and internal.

2.2.4. Qualitative Risk Defined Mathematically

Risk is the combination of the asset value, the vulnerabilities with respect to the asset, and the threats that can exploit the vulnerabilities. If all are high, then the risk is high. If all are low, then the risk is low. Conversely, the asset may be very valuable but the vulnerability may be exceedingly low. To define risk mathematically:

Relative **R**isk **= A**sset Value **x V**ulnerability **x T**hreat

So, getting back to our original example, leaving money in the park was risky because we put a valuable asset (money) in a vulnerable situation (wide open and easily accessible) where there were threats (anyone and anything in the park). Each value was high, therefore the risk was high.

Asset Value (**High**) x Vulnerability (**High**) x Threat (**High**) = **High Risk**

In contrast, if you were to leave an empty bag of chips on the ground, it is doubtful that anyone would take it and, if they did, your loss would be minimal. Thus, this would be a low risk (notwithstanding environmental concerns due to littering.)

Asset Value (**Very Low**) x Vulnerability (**High**) x Threat (**High**) = **Low Risk**

Thus, if undertaking an activity makes an asset vulnerable and there are threats that can exploit the vulnerabilities, then there is risk. The valued asset in the first example was money, the vulnerability was leaving the money in a public place, unprotected and in clear view, and the threat was anyone who could take the money. Note in the empty bag of chips example that the only thing that changed was the asset value (a bag of chips rather than two hundred dollars.) The vulnerability and threat did not change. However, because the asset was essentially worthless, the risk was lower. If the vulnerability or threat had been lower instead, the risk still would have been lower. Thus all three inputs to risk – asset value, vulnerability, and threat - contribute to the level of risk associated with a given activity or situation.[1]

2.2.5. Risk Tables/Matrices

There are typically multiple vulnerabilities associated with an asset and multiple threats that can exploit vulnerabilities. For example, money (in the park example) can be stolen, it could blow away so that we can't find it, or an animal might take it (for some unknown reason). In each case, the vulnerability is the complete lack of protection, but the threats are humans, the wind, and the wild.

Risk$_1$ = Asset (**Money**) x Vulnerability (**Exposed**) x Threat (**Stolen**)
Risk$_2$ = Asset (**Money**) x Vulnerability (**Exposed**) x Threat (**Wind**)
Risk$_3$ = Asset (**Money**) x Vulnerability (**Exposed**) x Threat (**Wild**)

This is a simple example, but in information systems the number of assets and their corresponding vulnerabilities and threats can grow quite large. For this reason, a matrix (a table) or matrices of risks must oftentimes be created to view and manage the volume of risks.

3. The Value of Assessing Risk

Why is it important to understand risk? In the context of information systems, the assessment and mitigation of risk makes the following things possible.

3.1. Identification of Security Gaps

There may be gaps in policy, process, infrastructure, applications, etc. Sometimes the risk assessment of one system results in the revelation of far greater and systemic gaps in the information security of the organization. For instance, an application and its

[1] Unknown Author. "Introduction to Risk Analysis"

associated hardware may be well-secured in terms of access controls, but be highly vulnerable due to weak human processes for granting access after the system has been installed. This same weakness could also impact all applications and servers and thus greatly diminish the overall security posture of the organization.
Another potential and far-reaching gap is a lack of security policy. When people don't know what's expected of them in terms of security, the results are unpredictable and no one can be held accountable. Thus, a risk assessment can be used to identify large gaps in an organization's security posture in a way that will have credibility with non-technical decision makers.

3.2. Costs versus Benefit

It is quite typical for organizations to give lip service to security, while in practice do only the minimum required to get by (if that). This is due in part to a lack of understanding of the costs and benefits of implementing security. Risk assessments help to make the bottom-line impact of security accessible to non-technical decision makers. When they can see for themselves what the impacts of various decisions will be, they can make better decisions and know why they're making those decisions.

3.3. Credibility and Pertinence

Although it is often difficult to provide hard numbers on cost versus benefit, which would make it easier to justify security recommendations, risk assessments are typically done with or by the decision makers in a facilitated manner which enhances their personal investment in security and their feeling that it will be pertinent to their needs. They provide the input that indicates which assets are most important and what the impact would be if various adversities befell them. This involvement in the process of risk assessment makes decision makers more willing, if not quite willing, to implement the recommendations that they helped to produce. Facilitated risk assessment, at least during the asset and asset value identification phase, helps decision makers feel that security is in tune with the organization's needs and that security is actually a business issue and not just a technical one. Thus, risk assessments can raise the credibility of a security department's recommendations and purpose within the organization, especially in environments where there is little mutual understanding of what the two have to offer each other.

3.4. Prioritization of Risks

There are typically many vulnerabilities and threats to the assets of the average mid-sized to large organization. (Some small organizations have this problem too, but it's more common at larger organizations.) Without a tool to identify, rate and compare risks, it's not likely that all of the most important risks will be mitigated and it is likely that less important risks will receive a disproportionately large share of attention and resources.

3.5. Expert Results without Experts

Some risk assessment methodologies available make it possible for a non-expert to take advantage of expert knowledge and produce a fairly credible measure of the most important risks facing the organization's information assets. One doesn't have to start

from scratch or guess at what the right questions are nor guess again about what the answers mean. Methodologies are available which can analyze the results of a risk assessment and make intelligent recommendations for action based on industry best practices. Some methodologies have been made into programs which come with questions, analysis code, and automated reports based on the responses.

4. Overview of Risk Assessment

4.1. Standard Pattern of Risk Assessments

Most of the risk assessment methodologies contain all or most of the elements below even though some are quite different from the others. By enumerating and briefly describing each element, one can get a sense of how risk assessment is done in general that will create a basis for understanding the variations.

- Identify and Assign Values to Assets
- Identify Exposure / Vulnerabilities, Threats and Controls
- Assess Risks for each Asset
- Create Action Plan

4.1.1. Identify and Assign Values to Assets

Both quantitative and qualitative methods identify and seek to assign either specific or relative values for assets. This is typically a first step in any risk methodology because the protection of assets is the basis for security, and no action can be taken unless something is at risk.

4.1.2. Identify Exposure / Vulnerabilities, Threats and Controls

The next step is to identify exposure or vulnerabilities, threats and controls. Some methods use facilitated sessions with experts to determine the vulnerabilities and threats and some use automated tools. Some use standard questionnaires while some do not. And some, of course, use combinations. In a quantitative risk analysis, the vulnerability and threats combine to determine the Exposure Factor. In qualitative analysis, the entire value of the asset is considered to be at risk (as opposed to its exposed percentage), but one can divide assets into small enough portions so that this is not a gross inaccuracy. An example of this might be a single field in a database containing customers' social security numbers as opposed to all fields in the database.

4.1.3. Assess Risks for each Asset

This step builds on the previous two to determine which risks are greater or less than others. In some methodologies, this is a manual process. In others, this is completely automated. However it happens, this is the step that determines which risks are greatest and thus which should receive the most attention. In quantitative risk analysis, this should produce ALE values. In qualitative risk analysis, this would produce risk profiles or tables of relative risk with respect to assets.

4.1.4. Create Action Plan

In this step, the results of the risk analysis are transformed into a plan for action. This can lead to new security policy, procedures, technical guidelines, or immediate action in the form of a project.

5. Risk Assessment Methodologies

5.1. Quantitative Risk Methodologies

Although there are many well-developed industries that use quantitative risk, it is not commonly used in information technology. In fact, it is very rare indeed.[1] However, risk methodologies can be partially quantitative and partially qualitative. It is the position of this author however to categorize all of the major methodologies as essentially qualitative because none of them can produce ALEs that can credibly be used to measure *specific* costs versus benefits as quantitative risk analysis should. They instead provide a more general sense of cost versus benefit despite sometimes having aspects which are predominantly quantitative, such as incident statistics.

5.2. Qualitative Risk Assessments

The following are some of the major risk assessment methodologies available today.

- COBRA
- OCTAVE®
- FRAP
- SPRINT, SARA, FIRM

Some are publicly available (e.g. OCTAVE), while others are restricted to members of organizations that are collaborating to create and updated them (e.g. SPRINT). The following are brief descriptions of each of these methodologies.

5.2.1. COBRA

http://www.riskworld.net/

COBRA stands for Consultative, Objective and Bi-functional Risk Analysis. It was created around 1991 by C & A Systems Security Ltd., based in the United Kingdom. COBRA was designed to give organizations the means to perform a self-assessment of their security posture, which includes risk assessments, without the need for external assistance from consultants. It also seeks, as most risk assessment methodologies do, to help businesses view security as a business issue rather than primarily as a technical one and one which can and should be justified in terms of costs and savings.

COBRA follows the guidelines set forth by ISO 17799, and its methodology is not so much a documented process as a downloadable program that consists of two major parts: Risk Consultant and ISO Compliance. Both sub-applications are customizable and utilize knowledge bases containing expert knowledge to aid the user in analyzing their security risk. The user can construct custom questionnaires based on templates

[1] Jacobson, Robert. "Quantifying IT Risks"

and then use the questionnaire to build a response set. The responses can be changed at a later point to view the impact of variations, and COBRA can produce reports which review and summarize the data and which provide recommendations based on best practices.

Risk Consultant, briefly, comes with standard questions for gathering the types of assets, vulnerabilities, threats, and controls that are in place in an organization. It is able to use the responses provide to produce an analysis of the risks, including what-if scenarios, and is able to produce recommendations for action. [1] ISO Compliance comes with standard questions which assess the major categories specified in the ISO 17799 standard. As with Risk Consultant, it can provide an assessment of an organizations compliance and suggest steps for action. [2]

5.2.2. OCTAVE®

http://www.cert.org/octave/omig.html
OCTAVE® stands for Operationally Critical, Threat, Asset and Vulnerability Evaluation. It was created at the Software Engineering Institute (SEI) at Carnegie Mellon University, a federally funded (DoD) research and development center.

OCTAVE® is a set of criteria that can be used as the basis of a methodology. Thus, the OCTAVE® Method is a manifestation of the OCTAVE® Criteria, and any other methodology that conforms to the OCTAVE® Criteria could be expected to produce similar results. The criteria specifies that a skilled analysis team, made up of people within an organization, gather input from the organization, analyze the results and act upon them in a structured and methodical manner. This process is aided by the use of the Catalog of Practices, which is similar in concept to some of the expert knowledge provided with COBRA. The process flow is similar to the general flow mentioned above:

- Phase 1: Build Asset-Based Threat Profiles
- Phase 2: Identify Infrastructure Vulnerabilities
- Phase 3: Develop Security Strategy and Plans

Phase 1: Build Asset-Based Threat Profiles
The analysis team meets with members of the organization from the top to the bottom to identify assets, vulnerabilities, threats, and current controls.

Phase 2: Identify Infrastructure Vulnerabilities
The analysis team expands on phase 1 by analyzing the key infrastructure associated with the assets identified and searching for vulnerabilities.

Phase 3: Develop Security Strategy and Plans
At this stage, the risks associated with the assets are assessed and a plan for action is begun. As with all risk assessment methodologies, OCTAVE is just one piece of a larger security strategy. So, although it can be leveraged to produce a plan for action, the execution of that plan and subsequent steps are not in its scope. [3]

5.2.3. FRAP

http://www.peltierassociates.com/frap.htm
FRAP, or Facilitated Risk Assessment Process, was created by Thomas Peltier, a prolific and respected author and educator in the area of information security. FRAP is designed to enable an organization to use its own people to facilitate the main steps involved in risk assessment much as the others are. FRAP fully situates itself in the qualitative camp and basically conforms to the standard pattern of risk assessment for qualitative risk. Thomas Peltier has published a book on FRAP, titled Information Security Risk Analysis, and it appears to be the least costly method to gain additional information on this methodology. Several firms, including RSA, teach the FRAP method. [4]

5.2.4. SPRINT and SARA

http://www.securityforum.org/ReportsLibrary2002/categories/cat/risk.htm
The Information Security Forum is a not-for-profit organization that, in its earlier incarnations, was formed to assess network and computer security on behalf of the European Commission. Today, it's an international organization that creates standards and performs research on behalf of its members who fund it. The standards and information that it produces are meant to only be accessible to its members, so, although detailed information is available about these methodologies (SPRINT and SARA), it will not be included here. To summarize them briefly, SPRINT is a **S**implified **P**rocess for **R**isk **I**de**NT**ification. This methodology follows the previously provided template for risk assessments very closely. SARA, **S**imple to **A**pply **R**isk **A**nalysis for information systems is supposed to provide more rigor than SPRINT for efforts that have been determined to involve more complexity or risk. [5]

6. Conclusion

Information risk is still a relatively immature and evolving field within information security and information systems. This may account for why all of the major methodologies are qualitative and not quantitative, which would allow for cost/benefit analyst. Nonetheless, good results can be obtained with these methods. It is the author's hope and expectation that this field will continue to evolve and eventually be able to obtain the Holy Grail of quantitative assessment while also delivering the insight and nuance that is characteristic of qualitative analysis. Risk and risk assessments are a key piece of any successful, comprehensive security strategy. They substantially help in determining what is most valuable and at the most risk, and can often help to determine what must be done to reduce those risks. They also help to ensure that security is effective and is aligned with the organization's goals. Therefore, there is clear value in taking advantage of this capability.

In conclusion, this paper has sought to explain 1) what risk is, 2) why it is useful, 3) types of risk and risk assessments, and finally 4) it has sought to expose the reader to several of the risk assessment methodologies available. At the same time, it has sought to avoid complexity or excessive detail so that this information is readily accessible to the average reader. Hopefully, it has done this successfully and the

reader can profitably use this knowledge as the basis for the pursuit of additional information as it pertains to his or her needs.

7. References

Van Scoy, Roger L. *Software Development Risk: Opportunity, Not Problem.* Software Engineering Institute, CMU/SEI-92-TR-30, ADA 258743, September 1992

Query for "risk". Dictionary.com.
URL: http://www.dictionary.com (7/29/03)

Horton, Thomas. "Managing Information Security Risks - Part 2". IT Audit. 15 October, 2000.
URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=256 (6 Aug. 2003)

Unknown Author. "Introduction to Risk Analysis". C & A Systems Security
URL: http://www.security-risk-analysis.com/introduction.htm (6 Aug. 2003)

Unknown Author. "Introduction to Security Risk Analysis". C & A Systems Security.
URL: http://www.security-risk-analysis.com/ (7/29/03)

[1] Unknown Author. "Features". C & A Systems Security.
URL: http://www.riskworld.net/advantages.htm (6 Aug. 2003)

[2] Unknown Author. "ISO 17799". C & A Systems Security.
URL: http://www.riskworld.net/7799.htm (6 Aug. 2003)

Jacobson, Robert. "Quantifying IT Risks". ITAudit. 15 August, 2002.
URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=479 (6 Aug. 2003)

[3] "Information Security Risk Evaluation". Carnegie Mellon SEI. 23, June 2003.
URL: http://www.cert.org/octave/ (6 Aug. 2003)

[4] Peltier, Thomas. "Peltier Associates Facilitated Risk Analysis Process (FRAP)".
URL: http://www.peltierassociates.com/frap.htm (6 Aug, 2003)

[5] "Information Risk Management". Information Security Forum. June 2002.
URL: http://www.securityforum.org/ReportsLibrary2002/categories/cat/risk.htm (6 Aug, 2003)