

## *Chapter 4*

# Other Qualitative Methods

To date, no one risk analysis technique has been created that will satisfy the needs of every enterprise. This chapter reviews a number of risk analysis techniques, which, combined with the material presented thus far, provides a number of alternatives from which to choose.

Thus, to reinforce the risk analysis process, this chapter examines variations on the theme established in Chapter 1. By examining the different methods and processes, the reader will be able to blend his or her own special risk analysis process. Chapter 5 examines the Facilitated Risk Analysis Process (FRAP) and Chapter 6 discusses variations on the FRAP theme.

This chapter examines five different risk analysis processes:

1. vulnerability analysis
2. hazard impact analysis
3. threat analysis
4. questionnaires
5. single-time loss algorithm

## **Vulnerability Analysis**

This form of risk analysis was presented to the computer security community by Donn Parker and is a process that analyzes the vulnerabilities of a department with respect to the people who work there. The process examines the jobs involved, the skills required to perform those jobs, the current working conditions, and the adequacy of controls.

A vulnerability analysis is normally conducted to see the current level of conditions, and then six to nine months later to determine how the new controls are working. To begin the process, first identify the occupations or job classifications being used within the target area. The target area can be as small as

a workgroup or as large as a division or business unit. The process works best if copies of the job descriptions and a current organization chart are available. Review all of the tasks being done and link them to specific job classifications.

The second step is to finalize the scope of the review. It could be the effects of certain job classification levels on controlling access to sensitive information, or the security of a specific LAN on the corporate network or a specific application. There are two main points to understand when discussing scope and vulnerability analysis. First, it is vitally important to properly describe exactly what is being reviewed. As discussed in previous chapters, the key to a successful risk analysis is to have the scope statement correct. Second, the only restriction placed on what can be reviewed is one's imagination or enterprise needs.

Take a minute or two to examine what topics might be a subject for a vulnerability review. As discussed above, the risk analysis could examine the effects of specific jobs on sensitive information. Thus, the scope statement might be "Review of Human Resources department handling of confidential information." To be successful in this review, one must have the definition of confidential information accessible to the vulnerability analysis team.

It is then necessary to identify the various job titles within the Human Resources department. These might include the following:

- vice president of Human Resources
- senior managers
- line managers (supervisors)
- senior specialists
- specialists
- recruiters
- diversity team lead
- office administrators
- contractors
- custodial staff
- vendors
- information systems support

Once all of the job titles have been established, it is necessary to have their job descriptions available to ensure each team member has the same understanding of the roles the specific job plays. For nonspecific activities such as contractor, vendor, or other third party, the team must develop an enterprisewide description that can be used in other reviews.

With the scope statement and the job titles, the last item the team needs to establish for the review is what effects need to be reviewed. Typically, for confidential information, a risk analysis will concentrate on:

- unauthorized access
- unauthorized modification
- unauthorized disclosure
- unauthorized destruction

**Exhibit 4.1 Vulnerability Analysis Worksheet**

**Scope** — Review of Human Resources department handling of confidential information.

<b>Occupation</b>	<b>Unauthorized Access</b>	<b>Unauthorized Modification</b>	<b>Unauthorized Disclosure</b>	<b>Destruction</b>
Vice president of HR				
Senior managers				
Line managers (supervisors)				
Senior specialists				
Specialists				
Recruiters				
Diversity team lead				
Office administrators				
Contractors				
Custodial staff				
Vendors				
Information systems support				

- 1 – Greatest risk
- 2 – Great risk
- 3 – Moderate risk
- 4 – Limited risk
- 5 – Low risk
- 6 – No risk

As with the job titles, it will be necessary to define what each of these review points means; that is, when reviewing “unauthorized access,” is the team to examine the job’s ability to gain access to confidential information in an unauthorized manner, or should one examine their ability to provide unauthorized access? These definitions need to be made prior to the start of the review.

Once completed, the Vulnerability Analysis Worksheet might look something like the one shown in Exhibit 4.1.

Using the materials discussed in Chapter 2 on the qualitative risk analysis process, the team will assess each job title on its effects on confidential information. The team is to rank each job from a high of Greatest Risk to a low of No Risk. This can be done in a number of ways. Each process, however, must begin with all team members understanding and agreeing with all definitions. Once that is accomplished, then the team can begin to work the analysis in one of three ways.

The first method is to have each team member do the analysis individually. Then, each of the scores are added together and divided by the number of

team members to obtain an average. Once this is complete, the team can discuss those job titles that had discrepancies. As with any qualitative risk analysis, it is the quality of the team that will lead to quality results.

Another method is to, as a team, review the job title for its impact on confidential information; this can be done by looking at each job one-by-one and determining its impact in each of the four categories. This requires that the team be together and that each process be discussed if there is any disagreement in the ranking. A variation on the second method, which looks across the worksheet horizontally, is to examine each category vertically; that is, at unauthorized access for each job title, then move on to unauthorized modification, etc. The correct way is the way that works best for one's enterprise.

This author has observed that some government agencies have a difficult time working a vulnerability analysis because every job is a greatest risk. That is correct if there are no controls in place. Even the most inefficiently run enterprise has some level of controls in place, even if they are only applied by individual departments or some employees.

This process will allow the review team to identify the level of risk associated with each job title and then propose controls that can help lower the risk level to an acceptable level. The review does not mean that any of these occupations would do anything unauthorized; but by understanding where the risks lie, effective controls can be put in place. The result of the vulnerability analysis is to identify a level of threat by job assignment. A blank Vulnerability Analysis Worksheet is provided in Exhibit 4.2.

## Hazard Impact Analysis

Where the vulnerability analysis looks at jobs and attempts to determine their impact to certain resources, the hazard impact analysis (HIA) was developed by the Federal Emergency Management Administration (FEMA) and the Michigan State Police to determine the hazards a site is most susceptible and vulnerable to experience. The process examines the types of hazards (normally natural threats), and the impacts to staff, property, and business. The process lends itself to those attempting to establish where limited resources are going to be spent to protect against some specific hazards.

Because it has been awhile since reviewing the standard set of processes in a risk analysis, take just a minute to review the basics:

1. Assemble the internal experts (the risk analysis team).
2. Develop a scope statement or risk analysis opportunity statement.
3. Agree on the definitions.
4. Ensure the team understands the process.
5. Conduct the risk analysis.

It is important that these steps be followed, regardless of what risk analysis process one decides to use or create. The results of one's work will be suspect if any of the steps are faulty.



When attempting to establish a list of appropriate threats, it is necessary to ask questions on how a specific threat might impact an organization. It is very important to consider threats, no matter how unlikely they may seem. Remember, a risk analysis is also a historical document that will allow others to see what threats were discussed and the reasons why they were deemed less important than others.

As discussed in Chapter 1, there are three basic elements that make up a threat. Generally speaking, these elements are:

1. *The agent*: the catalyst that performs the threat. The agent can be human, machine, or nature.
2. *The motive*: something that causes an agent to act. Breaking motive down by agent, the only one that can be both accidental and intentional is the human agent.
3. *The results*: for risk analysis team, the results would be an impact on the resources being reviewed if the threat were to happen.

There are factors that can impact the threats identified by the team. These include:

- *The organization's geographical location* — where you are located. Some areas of the world are impacted by the aging of the infrastructure that supports the business process.
- *The organization's operation facilities*. Older buildings have a tendency to have less adequate fire control systems in place and often the cabling need of information processing is inadequate.
- *The kind of information the organization processes or generates*. Financial institutions and those that provide services are always going to be targets for fraud.
- *The visibility of the organization*. This can be examined two ways. The physical visibility: can an outsider find the organization quickly? Is the facility one of the landmarks everyone uses for directions? "Oh, the shop you are looking for is just down the street from JR Enterprises." The other form of visibility is the profile of the organization. Some groups just do not like the way others earn their living or do not agree with their politics.
- *Emergency training for personnel*.
- *Employee morale*. Are all of the employees happy with their jobs, family, boss, and life? If so, this is probably one of the only enterprises where this might be true. No matter how hard an organization tries, there are always going to be some employees who have a morale problem.

Determining threats can be done in a number of ways, and many of these were discussed in Chapter 1. For the purpose of the HIA process, one can use the threats listed in Exhibit 4.3.

**Exhibit 4.3. Sample Threat Table**

Natural Threats	Accidental	Deliberate
Earthquake	Disclosure	Alteration of data
Flooding	Electrical disturbance	Alteration of Software
Hurricane	Electrical interruption	Bomb threat
Landslide	Emanation	Disclosure
Sandstorm	Fire	Sabotage
Snow/ice storm	Hardware failure	Fraud
Tornado	Liquid leakage	Riot/civil disorder
Tsunami	Human error	Strike
Volcanic eruption	Software error	Theft
Windstorm	Telecom interruption	Vandalism

### ***Hazard Impact Analysis Process***

Once the preliminary processes are complete, the team then examines each threat to determine probability of occurrence. As discussed above, the team must have a working definition of probability of occurrence and definitions of each threat. It is not sufficient to just have “fire” as a threat. There are at least three different levels of fire. To ensure that the team can give proper weight to each threat, the threat must be properly defined.

Using the worksheet displayed in Exhibit 4.4, the team examines each threat. In column **1** (Type of Threat), the team enters the types of threats:

- fire
- flood
- tornado
- virus
- fraud
- electrical outage
- bomb threat

Once those are entered, the team scores the probability of occurrence, either through group discussion and consensus or working individually and averaging the scores. The higher the number entered into column **2**, the higher the probability that the threat will occur. It might be necessary to provide guidelines for the numbering scheme, similar to what was done in Chapter 2. The team will want to concentrate on the threat and probability; the impact is reviewed later.

Once the probability has been established, the team next looks at impact. The effects of impact are divided into three categories:

- human
- property
- business



Each impact should be assessed individually, so it is probably better to review all Human impact elements and then move over to Property and finally Business. In reviewing impact, the team should address impact as if there are no controls in place. The controls come into play later. Once the impacts have been scored, the threat totals can be added and that figure entered into the **Sub Total** column (see Exhibit 4.5). A threat with a subtotal between 10 and 16 should be given extra attention.

The next area to be reviewed is resources that can lessen the impact of the threat. Note that these are reversed from the impact numbers. The team will want to identify existing internal controls that can help reduce the impact. This is a two-step approach: identify the safeguard resource and then determine its effectiveness in fighting the impact.

For example, in the threat of the Tornado, internal resources that could reduce the impact might be evacuation plans, evacuation drills, warning system (PA, alarm), or physical security staff monitoring weather bulletins. If there are internal controls in place, then the team enters their values in column **5**.

External controls for this scenario might include local tornado warning alarms, local weather bureau alerts, and building location. These two totals are then added to the **Sub Total** value (remember, they are reversed value: stronger is lower and weaker is higher), as shown in Exhibit 4.6. If there are no internal or external resources, then the value is 4.

The key to working with the HIA process is some common sense. The chances of a tornado hitting a building is very low; but if it does hit, then the impact will be very high. So, look for controls that will help, but that are also in line with reality. Save the budget for those threats that have higher probability and impact. Look at the recent virus attacks; none have been destructive, but they have been so persistent that the clean-up costs are now tagged in the billions.

## Threat Analysis

This is a variation of the HIA process just discussed. Instead of assigning a numeric value to a threat, the team attempts to determine how the threat might impact certain elements of the business process. In addition to the normal qualitative risk analysis first three steps (i.e., assemble the team, develop a scope statement, and agree on definitions), the team will identify those elements it wants to review. This is similar to what occurred in the vulnerability analysis process discussed earlier in this chapter. The team can look at as many or as few elements as it desires. In Exhibit 4.7, the Scope statement wants to review the effects of threats on the data center operation. The team has selected six elements to examine:

1. temporary interruption
2. temporary inaccessibility
3. hardware damage
4. loss of software
5. repairable damage
6. catastrophic damage

Exhibit 4.5 Hazard Impact Analysis Worksheet: Steps 1 through 4 Complete

Type of Threat	Probability	Human Impact	Property Impact	Business Impact	Sub Total	Internal Resources	External Resources	Total
	High Low 4← →1	High Impact	4← →1	Low Impact		Strong Resources 1←	Weak Resources →4	
Tornado	1	4	4	4	13			
Virus (benign)	4	1	1	2	7			
Electrical interruption	3	1	3	1	8			
<b>1</b>	<b>2</b>	<b>3A</b>	<b>3B</b>	<b>3C</b>	<b>4</b>	<b>5</b>	<b>5</b>	<b>6</b>

Note: The lower the score, the better.

**Exhibit 4.6 Hazard Impact Analysis Worksheet: Completed Example**

Type of Threat	Probability	Human Impact	Property Impact	Business Impact	Sub Total	Internal Resources	External Resources	Total
	High Low 4← →1	High Impact	4← →1	Low Impact		Strong Resources 1←	Weak Resources →4	
Tornado	1	4	4	4	13	2	2	17
Virus (benign)	4	1	1	2	7	2	3	12
Electrical interruption	3	1	3	1	8	2	3	13
<b>1</b>	<b>2</b>	<b>3A</b>	<b>3B</b>	<b>3C</b>	<b>4</b>	<b>5</b>	<b>5</b>	<b>6</b>

Note: The lower the score, the better.

**Exhibit 4.7 Threat Analysis Worksheet**

Potential Causes	Effects on Operations					
	Temporary Interruption	Temporary Inaccessibility	Hardware Damage	Loss of Software	Repairable Damage	Catastrophic Damage
LAN server outage	P	M				
Hardware failure	D	P	P	M		
Evacuation – bomb threat	D	M			M	M

Note: M – May affect.  
 P – Probably will affect.  
 D – Definitely will affect.

Using the scope statement and the elements to be reviewed, the team then identifies the threats to that resource and then determines if that threat:

- M = May affect
- P = Probably will affect
- D = Definitely will affect
- NA = Not Applicable, or can be left blank

The threat analysis process, like the others, can examine any number of elements. The risk analysis team is only restricted in what it can think of to review. Which method works best for a particular organization? That is a question one has to experiment with to determine what works best.

To make the last two risk analysis processes (hazard impact analysis and threat analysis), work best it will be important to ensure that the threats reviewed are actually threats that can impact the enterprise. Review the Scope statement and make sure it describes exactly what is going to be reviewed.

Once the analysis process is complete, the team must determine where additional controls are required, as well as develop a set of recommendations for the sponsor and management.

## Questionnaires

Another method of risk analysis is the development of a questionnaire. Questionnaires can be developed to meet a specific resources requirement or can be used to review a broader area. An important key to developing an effective risk analysis questionnaire is to remember the audience. Who will be filling out the forms? Will it be auditors, or security administrators, or managers? The level of the question language must meet the needs of the audience. The number of questions must also be limited.

Typically, a series of 20 questions per topic should be the outer limit. This is not a hard-and-fast rule, but the goal of a questionnaire is to get the user community to complete the document. When this author worked for a large multi-national corporation, the information security program was given 20 questions each year. Normally, they were divided into ten that usually remained constant and the other ten were used to assess the topic stressed that past year.

### *Risk Analysis Questionnaire Process*

Each question is reviewed for compliance to an existing enterprise policy, procedure, standard, or other regulation. If the reviewer answered YES, then in COMMENTS section, the reviewer should enter what methods were used to determine that the unit was in compliance with the question.

If the reviewer answered NO, then the COMMENTS section is used to identify the steps to be taken to move the unit into compliance, and by what date.

The DATE column is the date that the question was reviewed and the INITIALS are those of the reviewer (the individual who made the YES/NO determination).

On the final page of each questionnaire section, the business unit manager is required to sign. This is a way to ensure that the results have been reviewed with management. A typical questionnaire might look something like the one displayed in Exhibit 4.8.

A series of information security program questions might look like those listed in Exhibit 4.9.

The Computer Security Institute has prepared the Information Protection Assessment Kit (IPAK), which is a self-administered test intended to help an organization determine how well its information protection program is doing. The questionnaire was developed through the efforts of industry experts such as John O'Leary, CSI Director of Education; Cheri Jacoby, partner with Price-waterhouse Coopers, LLP; Dan Erwin, Information Security Specialist at Dow Chemical; Fred Trickey and Tom Peltier, Netigy Corporation; Mike Gregorio of the Coca-Cola Company; and Charles Cresson Wood, of Baseline Software. The IPAK is available through CSI for a nominal fee.

**Exhibit 4.8 Sample Risk Analysis Questionnaire**

Information Protection	Yes/ No	Comments	Date	Initials
1. A Corporate Information Officer (CIO) has been named and the CIO is responsible for implementing and maintaining an effective IP program.				
2. The Information Protection (IP) program supports the business objective and/or mission statement of the organization.				
3. An enterprisewide IP policy has been implemented.				
4. An individual has been assigned as the corporate information protection coordinator and overall responsibility for the IP program implementation has been assigned.				
5. The IP program is an integral element of sound management practices.				

**Single-Time Loss Algorithm**

John O’Leary, the Computer Security Institute’s Director of Education Resource Center, introduced the concept of the Single-Time Loss algorithm for risk analysis. This process takes some of the elements of quantitative risk analysis and adds some qualitative aspects.

O’Leary uses his background in mathematics to express the variables of a threat in a formula. The structure of this process is very similar to that of the methods examined heretofore. It requires that the key elements of risk analysis be done:

1. Assemble the internal experts (the risk analysis team).
2. Develop a scope statement or risk analysis opportunity statement.
3. Agree on the definitions.
4. Identify the threats.
5. Identify the requirements to recover from the threat.

## **Exhibit 4.9 Sample Information Security Program Questionnaires**

---

### **Information Protection Program and Administration**

---

1. A Corporate Information Officer (CIO) has been named and the CIO is responsible for implementing and maintaining an effective IP program.
  2. The Information Protection (IP) program supports the business objective or mission statement of the organization.
  3. An enterprisewide IP policy has been implemented.
  4. An individual has been assigned as the corporate information protection coordinator and overall responsibility for the IP program implementation has been assigned.
  5. The IP program is an integral element of sound management practices.
  6. IP is identified as a separate and distinct budget item (approximately 1 to 3 percent of the overall ISO budget).
  7. Senior management is aware of the business needs for an effective IP program, and is committed to support its success.
  8. An effective risk analysis process has been implemented to assist management in identifying potential threats, probability of threat occurrence, and possible countermeasures.
  9. IP controls are based on cost-benefit analysis utilizing risk analysis input.
  10. IP responsibilities and accountability for all employees with regard to IP are explicit.
  11. Each business unit, department, agency, etc. has designated an individual responsible for implementing the IP program for that organization.
  12. The IP program is integrated into a variety of areas, both within and outside the computer security field.
  13. Comprehensive information protection policies, procedures, standards, and guidelines have been created and disseminated to all employees and appropriate third parties.
  14. An ongoing IP awareness program has been implemented for all organization employees.
  15. A positive, proactive relationship with the audit staff has been established.
  16. Employees have been made aware that their activities may be monitored.
  17. An effective program to monitor IP program-related activities has been implemented.
  18. Employee compliance with IP-related issues is an annual appraisal element.
  19. The system development life cycle addresses IP requirements during the Initiation or Analysis (first) phase.
  20. The IP program is reviewed annually and modified when necessary.
-

This risk analysis process requires two brainstorming sessions: one to identify and prioritize the threats and another session to identify the recovery elements. The latter session may take longer than the first. For a threat like an earthquake, a completed algorithm might look something like the following:

$$\begin{aligned} &(\text{Total asset value} + \text{Contingency implementation costs} \\ &+ \text{Data reconstruction costs}) \times 0.25 + (\text{Cost of 1-week delay}) = \text{STL} \end{aligned}$$

This formula takes the value of the asset and adds that to the cost of implementing the business contingency plan plus the cost of data reconstruction. The determination of data reconstruction will include many factors, for example, the availability of backup media, the staff available to process the jobs, the new media to copy the backup to, and the time to do all of these tasks. The 0.25 that these figures are multiplied by is the annual rate of occurrence (as discussed in Chapter 1). Finally, the cost of one week's delay is added to these figures to give an STL total. The team must establish what a single day's loss to the enterprise might be. One way to do that is to take the annual revenues and divide that figure by 260 (the typical number of working days in a year), and this will give a ballpark figure on daily losses.

The algorithm represents those elements that would be necessary to recover a specific asset or resource if a certain threat was to occur. The formulas can be used in two ways: (1) the team can actually develop values for each element and work the formula, which might be a difficult task; or (2) the team can use the complexity of the formulas to help prioritize the threats and identify where safeguards will provide the most benefits.

## Conclusion

Which risk analysis process will work best for a particular person and a particular organization? Only that person/organization will be able to determine. Before this decision can be made, it will be necessary to examine as many as possible. This chapter has presented variations on qualitative risk analysis themes. The keys to each process are the same:

1. Assemble the internal experts (the risk analysis team).
2. Develop a scope statement or risk analysis opportunity statement.
3. Agree on the definitions.
4. Ensure that the team understands the process.
5. Conduct the risk analysis.

The next two chapters examine the Facilitated Risk Analysis Process (FRAP) and then three variations on this process to the reader in pre-screening application and conducting a business impact analysis.