หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

CHAPTER 2

INFORMATION SECURITY RISK ASSESSMENT

An understanding of risk and the application of risk assessment methodology is crucial to be able to efficiently and effectively create a secure computing environment. Unfortunately, it is getting challenging for information professionals as well as managers owing to the dizzy changes in technology, the relatively recent advent and explosive growth of the Internet and perhaps the prevalence of the attitude (or reality) that assessing risk is simply too hard to do. This has kept information systems and information systems security in undesirable position of being unable to systematically identify and manage 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 chapter 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?
- Why is an understanding of risk important?
- How is information understood to be 'secured'?
- What are the key elements of information security requirements?
- What is the importance of information security risk assessment?
- What are some of the common risk assessment methodologies?
- What are the OCTAVE^{SM} method and its characteristics? How are its procedures?

"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".
Van Scoy & Roger L.[16]

1. RISK, INFORMATION & INFORMATION SECURITY REQUIREMENTS

1.1 Risk

People may have an impression that risk is merely connected with statistics and probability lessons at school. Others consider risk as playing gamble in which luckiness usually dominate. Reality has, however, proved that correct and complete understanding of this concept may help reduce the level of uncertainties and give tie to prepare organizations for upcoming events.

The Oxford Advanced English Learner's Dictionary (2003) defined risk as followed:
"The possibility of suffering harm or loss; danger".

More formally, Stonebrunner, Gary, Alice and Alexis[17] defined:
"Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of the occurrence". Likewise, Christopher and Audrey believed that risk refers to a circumstance in which either somebody could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence.

Given the above definitions, it can be understood that risk is inevitable and that risk touches upon many aspects in daily activities of an organization – an event, uncertainty and a consequence. In the context of information security as similar as those illustrations in chapter 1, a basic event can be interpreted as a 'threat', uncertainty - which concerns whether a threat will develop as well as whether the organization is sufficiently protected against the threat or not - means 'probability' or 'likelihood of occurrence' and consequence - which ultimately maters in information security risk - can be understood as the 'resulting impact' on the organization due to a threat. Further study on other related aspects helps clarify the risk issue:

- *Asset:* Everything that has a value for an organization; For example: personnel records, printers, etc. In effect, threats directly exert influence on the asset but not organization.

- *Threats:* Potential causes of unwanted incident which can cause harm or loss for the system or organization; For example, a person uses network to access a database of an organization or fire destroyed a database system.

- *Vulnerabilities:* Weakness of an asset or a group of assets, which can be exploited by threats (ISO 13335-3: 1998[18]). More specifically, vulnerability is a weakness in the security system, for instance, in procedures, design or implementation, which might be exploited to cause loss or harm. As far as the threats and vulnerabilities are concerned, there goes another concept that cannot be failed to mention – *attack*. A human who exploits a vulnerability perpetrates an attack on the system. An attack can also be launched by another system, as when one system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function.

- *Outcome:* The negative consequences, which the organization experiences as a result of being vulnerable. According to Christopher and Audrey[8], there are four types of outcomes that are directly related to assets and describe the effects of the threat on an asset:
  - Disclosure of an asset
  - Modification of an asset
  - Loss/destruction of an asset
  - Interruption to an asset

  More discussion on how an asset is disclosed, modified, damages/lost or interrupted will be mentioned in section 1.3.

- Finally, it's the *control* that must be taken into account. We use *control* as a protective measure. A *control* is, as described by Charles and Shari[11], an action, device, procedure or technique that removes or reduces a vulnerability.

The figure below would provide us with better visualization of the chain: threat – vulnerability – consequence – control.

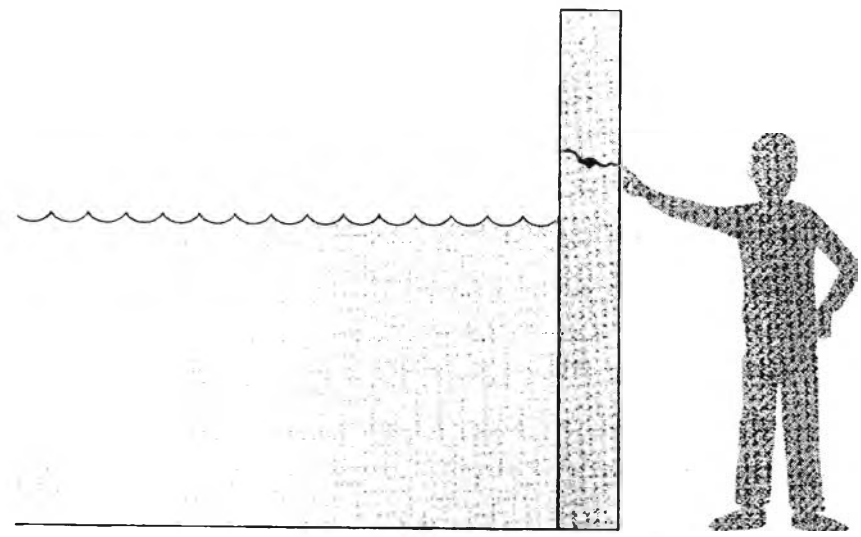

FIGURE 2-1: *Threat – Vulnerability – Consequences – Control. Adapted from Figure 1-1, p.6, Charles and Shari*[11].

In this figure, a wall is holding the water back. The water to the left of the wall, supposedly, is *a threat* to the man on the right of the wall: the water could rise, overflowing onto the man or it could stay beneath the height of the wall, pushing it to collapse. So the threat of harm is the potential for the man to get wet, get hurt or drown (*consequences*). Now, the wall is intact, so threat is unrealized (clearly).

However, there is a small crack in the wall – a vulnerability that threatens the man's security. If the water level is higher than that of the crack, it will exploit this vulnerability and harm the man. To control such a threat of water leakage, the man is temporarily putting his finger into the crack until he finds a more effective control (way) to this threat. Charles and Shari[11] concludes the relationship among threat, control and vulnerability in this way:

"A *threat* is blocked by a *control* of a *vulnerability*".

In a word, risk, the keyword of this study, is the primary concern of risk assessment. Exploring its model in depth will help select appropriate risk assessment approach.

1.2 Information

The concept of asset given by ISO 13335:3: 1998[18] seems to be broad. In this study, information is considered as an asset of the organization. There are many definitions regarding to information asset. For instance, information asset is something that is stored on paper or computer. Other people broaden such definition by including talk or communication or even ideas. All of those, in my opinion, are correct but not complete. It must be more systematic. As far as the context of information technology is concerned, anything related to information - according to Fites, Kratz and Brener; BSI; Hutt, Bosworth and Hoyt; Caelli, Longley and Shain (all cited from Christopher and Audrey[8]) - is considered asset including both logical and physical forms:

- *Information* – documented (paper or electronic) data or intellectual property used to meet the mission and objectives of an organization.
- *Systems* – information system that process and store information (systems being a combination of information, software and hardware assets and any host, client or server being considered a system).
- *Software* – software application and services such as operating systems, database applications, networking software, office applications, custom application, etc. that process, store or transmit information.
- *Hardware* – information technology physical devices such as workstations, servers, etc. that normally focus solely on the replacement costs for physical devices.
- *People* – the staff in an organization that possess unique skills, knowledge and experience that are difficult to replace.

As such, it can be deductive that an information security risk assessment must focus on an organization' information-related assets. Otherwise, the assessment method can easily overlook or miss few mission-critical objectives.

1.3 Information Security Requirements

Every organization, unarguably, has theoretical or practical weaknesses or both that might be exposed to threats. Therefore, the purpose of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents and violations. To understand what preventive measures make the most sense, let's find out what is a 'secure' system or organization.

To begin with, let me take an example of a house's 'physical security'. When we talk about this concept, we mean a house is protected in such a way that should an intruder attempts to get in, an installed 'automatic system' will immediately warn the neighbors or the police stations. Another example is 'financial security' in which a set of investments is adequately funded. Over time, such investments will grow so that we have enough money for other purposes later in life. Similar understanding goes to the phrase 'information security'.

According to ISO/IEC 17799: 2000[15] and Charles and Shari[11], information security is characterised as the preservation of:

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access; 'Access' here means not only reading but also viewing, printing or even simply knowing that a particular asset exists. Others terms related to *'confidentiality'* are *'secrecy'* or *'privacy'*.
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods; In other words, assets can be modified only by authorized parties or only in authorized ways. In this context, *modification* includes writing, changing, changing status (i.e. fabricating), removing, deleting and creating.
- **Availability:** ensuring that authorised users have access to information and associated assets when required. In other words, if a party has legitimate access to a particular asset, that access should not be prevented or *interrupted*. On the contrary to 'availability' is the term 'Denial of service' (DoS).

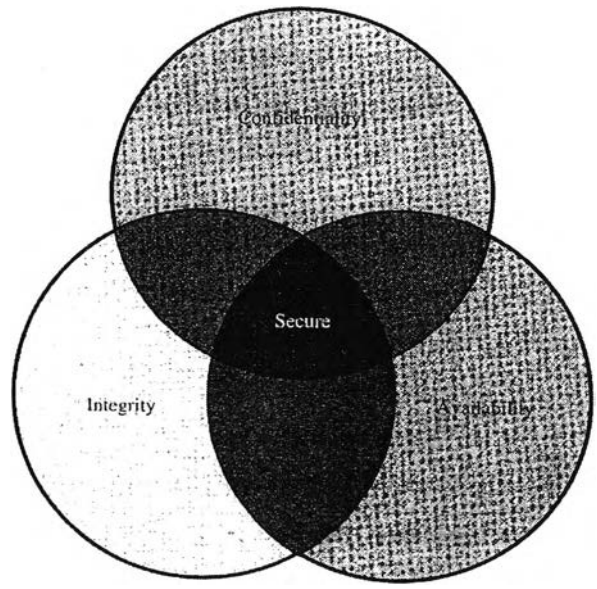

FIGURE 2-2: *Relationship between Confidentiality, Integrity and Availability. Adapted from Figure 1-3, p.11, Charles and Shari*[11].

It is required that information security addresses these three goals. Yet, one of the challenges in setting up a secure system or organization is to properly balance the relationship among these goals, which easily lead to conflict. For example, for confidentiality of a particular asset, it's tempting to prevent everyone from seeing or accessing it. When doing so, however, the owner of the system or organization violates the third requirement – 'availability'. This conflict reveals the fact that a balance between 'confidentiality' and 'availability' is a must.

As information is increasingly being processed and stored in a technological environment, in addition to the three widely-accepted requirements above – as identified by Lim, Kwan and Alvin[20] - the following security requirements pertaining to IT are also important:

- **Non-repudiation:** ability to prove an action or event has taken place, so that this event or action cannot be repudiated later; This requirement, in my opinion, can be especially significant in many large-scale organization or system which run numerous processes. It helps to reduce time for checking.
- **Accountability:** the property that ensures that the actions of an entity may be traced uniquely to the entity; This requirement aims at monitoring business transactions on the network. It helps to quickly identify problems of a system during operation, which is usually time-consuming.

- **Authenticity:** the property that ensures that the identity of a subject or resource is the one claimed; This requirement is, in my opinion, much supportive to 'confidentiality' and 'integrity', which require the true 'identity' to view or modify information assets.
- **Reliability:** the property of consistent intended behaviour and results. This requirement, in my opinion, is quite interesting and useful since it aims at enhancing the stability of a system or organization during operation. Any deviant behaviour or uncommon action is timely identified.

To this point, I have reviewed risk, information assets and information security requirements. I'll go farther to exemplify how the above-mentioned information security requirements can be applied for each information asset. According to Christopher and Audrey[8]:

- *For information assets,* the security requirement will focus on the confidentiality, integrity and availability of the information. For example:

  ⇒ The information must not be viewed (disclosed) by unauthorized personnel (confidentiality);

  ⇒ The information can be modified only by authorized personnel. Furthermore, it must not be fabricated (integrity);

  ⇒ The information must be available whenever requested. More clearly, access to information cannot be interrupted or intercepted (availability);

- *For system assets,* the specific aspect or quality of the system that is important will drive the security requirements. There are two cases to be considered:

  If the information stored, processed and transmitted by the system is the most important aspect, then:

  ⇒ The information on system ABC must not be viewed (disclosed) by unauthorized personnel (confidentiality);

  ⇒ The information on system ABC can be modified only by authorized personnel. In addition, it must not be fabricated (integrity);

  ⇒ The information on system ABC must be available whenever requested. More clearly, access to the system ABC cannot be interrupted or intercepted. Downtime for system ABC can be only 15 minutes every 24 hours (availability);

  If the service provided by the system is the most important aspect, then:

  ⇒ The service provided by the system ABC must be complete and consistent (integrity);

หอสมุดกลาง สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

⇒ The service provided by the system ABC must be available whenever requested. Access to the system ABC cannot be interrupted or intercepted. Downtime for system ABC can be only 15 minutes every 24 hours (availability);

- *For software asset,* attention is paid to the software application or service. Information that is processed, transmitted and stored by the application is beyond our concern. If the software is freely or commercially available, the confidentiality may not be applied. Otherwise, confidentiality must be mentioned. For example:
  ⇒ Application XYZ must not be used by unauthorized personnel (confidentiality);
  ⇒ Application XYZ can be modified only by authorized personnel. Besides, it must not be fabricated (integrity);
  ⇒ Application XYZ must be available during normal working hours. More clearly, it must not be interrupted, deleted or intercepted (availability);

- *For hardware assets,* it is suggested to focus on the physical hardware when identifying security requirements. Attention should not be paid to information processes, transmitted and stored by the hardware. Confidentiality generally does not apply to physical hardware. Modification of a hardware asset focues on adding or removing hardware (e.g. removing a SCSI drive or adding an ADSL modem). Availability focuses on whether the asset is physically available or accessible. For example:
  ⇒ The hardware can be modified (substituted) only by authorized personnel. Moreover, it must not be fabricated (integrity);
  ⇒ The hardware must be accessible to authorized personnel during normal working hours. More specifically, it must not be interrupted due to Denial-of-Service attack (DoS) or intercepted due to theft (availability);

- *For people assets,* it is suggested to focus only on availability requirement. It's noteworthy that people are a special case. When they are identified, it is because of their skills and expertise or because of services provided by them. Thus, availability of the service or asset is our primary concern. For example:
  ⇒ The IT staff must provide ongoing and consistent system and network management services (availability).

For convenience, the above plain text will be transformed into five diagrams.

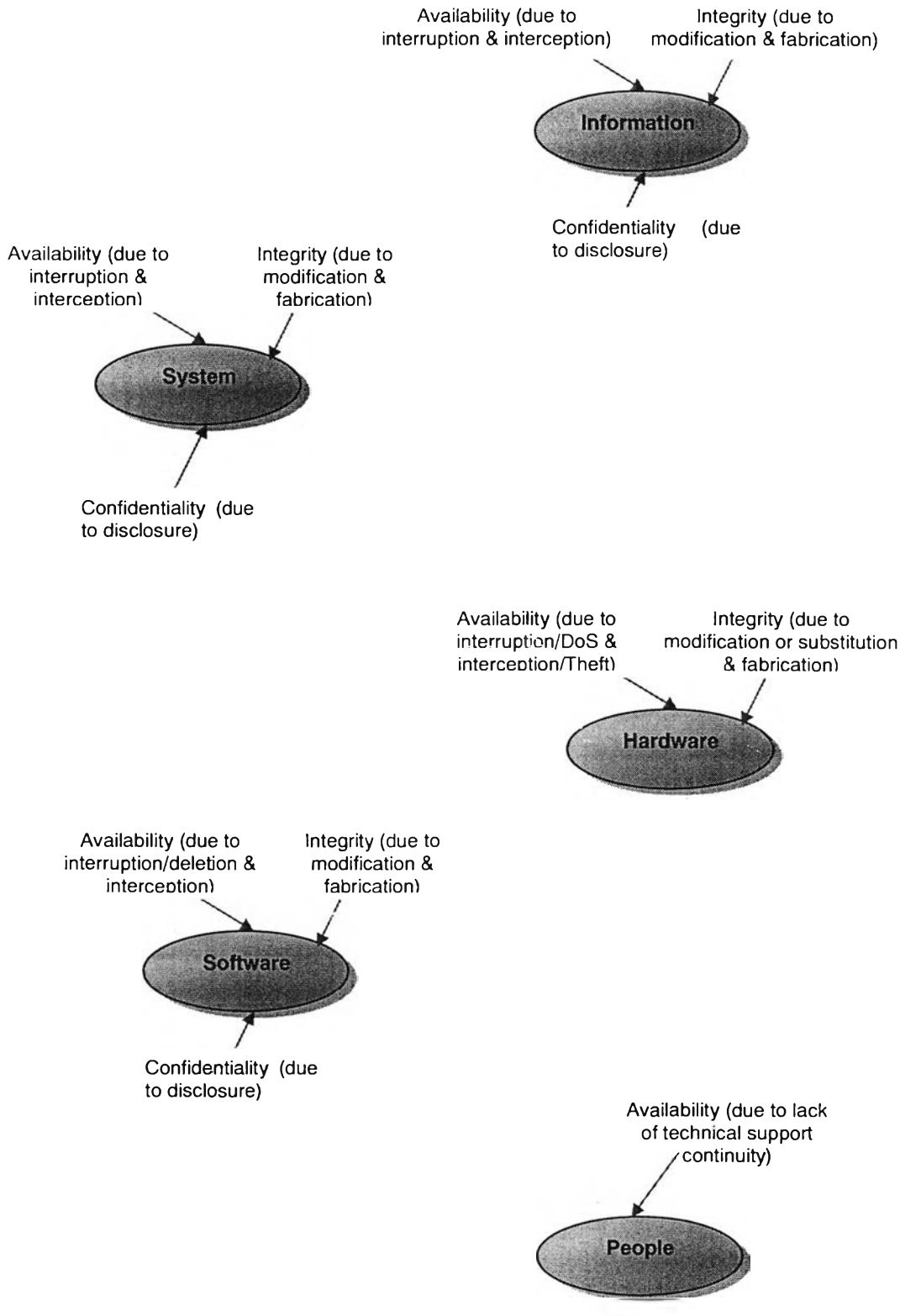

FIGURE 2-3: *Information Security Requirements for Information Assets in Organization*

2. INFORMATION SECURITY RISK ASSESSMENT

Risk assessment – an indispensable and critical part of an efficient ISMS – also brings us other benefits that cannot be failed to mention. Exploring these benefits is significant for not only senior managers but also information professionals.

2.1 The Importance of Information Security Risk Assessment

- ***Identification of security gaps***

Understandably, there may be gaps in policy, process, infrastructure, applications, etc. Sometimes the risk assessment of one system, as Vishal[20] explained, results in the revelation of gaps in the information security of the organization. For instance, an application and its associated hardware may be well-secured in terms of access controls, but be highly vulnerable due to a weak granting access after the system has been installed. This weakness could, in my opinion, impact all applications and hardware and thus greatly diminish the overall security posture of the organization. Vishal also pointed out another potential and far-reaching gap - a lack of security policy. He explained that 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. Given his experiences, I would think that a risk assessment could be utilized to identify large gaps in an organization's security posture in such a way that will have credibility with senior management.

- ***Costs and benefit – B/C (Return on Investment - ROI)***

Costs and benefit (B/C) or Return on Investment (ROI), in my opinion, is not unfamiliar but decisive issue not only in project management but in information technology as well. Indeed, it is observed that just few organizations seriously dedicate their efforts whilst others potter at information security practices (Karnjana[5]). This fact is attributed to the lack of understanding of the costs and benefits of implementing security (Vishal[20]; Christopher and Audrey[8]). Deducing from this argument, I would think that risk assessment is very supportive to senior management as they themselves can see the bottom-line impact of various decisions on information security practices. Only then can they make their IT investment more effective and convincing.

- ***Credibility and pertinence***

Risk assessment, at least during the asset and asset value identification phase, helps senior management feel that security is in tune with the organization's needs and that security is actually a business issue, not just a technical one (Ding[21]). Thus, risk assessments can raise the credibility of an IT department's recommendations and purpose within the organization, especially in the environment where there is little mutual understanding among many divisions as well as levels.

- ***Prioritization of risks***

There are typically many vulnerabilities and threats to the assets of an organization. Without a tool to identify, rate and compare risks, it's highly unlikely that almost important risks will be mitigated and it's tempting that less important risks will receive a disproportionately large share of attention and resources. This benefit can be easily seen when I implement the OCATVE[SM] method in Chapter 4.

2.2 Strategies for Information Security Risk

During a Microsoft conference in Warsaw, Finland, Mr. Jedynak[22] explained risk strategy as followed:

"Imagine that we want to buy a car, but we are afraid it might be stolen. Of course we can do nothing, accept the risk and let the car stay unprotected at the parking place. We can as well try to reduce the risk by installing auto protection systems like auto alarm or GPS. Next thing we can also try to do is to transfer the risk to an insurance company by buying appropriate insurance. And finally we can completely avoid the risk by not buying car at all".

The above-illustrated story reveals the fact that organization must face with risk nowadays in their appropriate way. Likewise, to deal with information security risk, there are 4 different ways to be taken into account: (Charles and Shari[11]; URL: http://www.ist-usa.com/aboutcora.htm[42]):

- *Avoidance:* by changing requirements for security or other systems characteristics.
- *Transfer:* by allocating the risk to other systems, people, organizations or assets; or by buying insurance to cover any financial loss should the risk become a reality.
- *Reduction:* by controlling it with available resources (i.e. staff, time, money, etc.) and preparing to deal with the loss if it occurs.
- *Acceptance:* by doing nothing.

In this study, certainly, the target of an efficient ISMS is nothing other than securing the information assets. Therefore, given those four strategies, either accepting risk (with low impact) or reducing risk (with high impact) would be the selection.

3. CURRENT INFORMATION SECURITY RISK ASSESSMENT APPROACHES

According to Vishal[20], risk, at its most fundamental, is an acknowledgement of the fact that life is uncertain and that there are variables both within and beyond of our control and awareness that are decisive to the consequences. In addition, 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. Perhaps, in my opinion, the two primary ways that risks are measured - quantitative and qualitative – will somehow reflect Vishal's viewpoints.

3.1 Quantitative Risk Assessment Methodology

Although there are many advanced industries that utilize quantitative risk assessment, it is not commonly used in information technology. In fact, it is very rare indeed (Jacobson[23]). Quantitative risk measurement is the standard way of measuring risk in many fields, such as finance and insurance, but it is not commonly used to measure risk in information systems. Two of the reasons claimed for this, according to Horton (cited from Vishal[20]) are: 1) the difficulties in identifying and assigning a value to an asset and 2) the lack of statistical information that would make it possible to determine frequency. Let me go further to clear the points. First, identifying and assigning value to some assets such as people or information (sensitive or confidential data) is full of challenges, especially in large-scale, dispersed organizations. Obviously, back to the definition of information asset in Section 1.2, it's hard to estimate the value of people in terms of their knowledge and expertise. Likewise, data regarding to national security or new product are ultimately incalculable. Equally and more difficult is determining statistical data on the likelihood of information security incidents and breaches due to the lack of condition for full observation (I would spend a little bit more space to discuss about this issue in the OCTAVE^{SM} method hereafter). Given those arguments, it's not surprised to know that most of the risk assessment tools that are used today for information systems are measurements of qualitative risk or a technique, namely scenario planning. Still, a preliminary review of this methodology would reveal the distinct advantages and the arguments of why qualitative approach for information system is preferable.

Quantitative risk assessment 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 would be called Return on Investment analysis (ROI) which is a common way to decide to take a certain action or explain why not to take it. Mathematically, quantitative assessment can be expressed as Annualized Loss Expectancy (ALE) equation:

ALE = Asset Value x Exposure Factor x Frequency,

in which *Exposure Factor* is the percentage of asset loss caused by identified threat; It ranges from 0% to 100% whilst *Frequency* is annual rate of occurrence

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.

3.2 Qualitative Risk Assessment Methodology

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 Control. It's noteworthy that the exposure factor is not present. This information is not assumed to be available, so vulnerabilities and threats are introduced instead. These values help to establish which risks are greater than others. Controls will be discussed later. As a simple illustration, let's say an IT staff wanted to keep his hard-disk, whose information is staff's salary and product information, safe by leaving it on the table in a reception-room. Obviously, this isn't a good idea, but it is risky so we can work with it. This example contains three of previously mentioned elements of risk, namely: assets, threats, and vulnerabilities.

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 the risk mathematically:

Relative Risk = Asset Value x Vulnerability x Threat

So, getting back to our original example, leaving a hard-disk in a reception-room was risky because we put a valuable asset (data) in a vulnerable situation (wide open and

easily accessible) where there were threats (anyone and anything in that place). Each value was high, therefore the risk was high.

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

In contrast, if we were to leave a totally damageable blank hard-disk at the same position, probably, anyone would take it and if they did, our loss would be minimal. Thus, this would be a low risk.

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

To summarize, if undertaking an activity makes an asset vulnerable and there are threats that can exploit the vulnerabilities, then there is risk. The valuable asset in the first example was a hard-disk, the vulnerability was leaving the hard-disk in a public place, unprotected and in clear view, and the threat was anyone who could take that hard-disk. Note in the second example that the only thing that changed was the asset value (a totally damageable blank hard-disk). The vulnerability and threat did not change. However, because the asset was essentially worthless, the risk was much 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 (Vishal[20]; URL:http://www.security-risk-analysis.com/introduction.htm[43]).

Such a qualitative background is merely an initiative. Different assessors with a variety of points of view develop different risk models. Here are a few risk assessment models that deploy the qualitative approach as followed:

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

Some risk assessment models are commercially available (e.g. OCTAVE) whilst others are restricted to members of organizations that are collaborating to create and update them (e.g. SPRINT).

- ***COBRA***

COBRA stands for Consultative, Objective and Bi-functional Risk Analysis created by C & A Systems Security Ltd., UK around 1991. 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 firms view security as a business issue rather than primarily as a technical one. Furthermore, it can 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 consisting 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. Users can construct their own questionnaires based on templates and then use the questionnaires to build a response set. The responses can be changed later to view the impact of variations and COBRA can produce reports, which review and summarize the data and 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 provided to produce an analysis of the risks, including what-if scenarios, and is able to produce recommendations for action. ISO Compliance comes with standard questions, which assess the major categories specified in the ISO 17799. (URL:http://www.riskworld.net/advantages.htm[44]). As with Risk Consultant, it can provide an assessment of an organization compliance and suggest steps for action.

- ***OCTAVE^{SM}***

OCTAVE^{SM} 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 research and development center (URL:http://www.cert.org/octave/[37]). OCTAVE^{SM} is a set of criteria that can be used as the basis of its methodology. Hence, the OCTAVE^{SM} method is a manifestation of the OCTAVE^{SM} criteria and any other methodology that conforms to the OCTAVE^{SM} criteria could be expected to produce similar results. The criteria specifies that a skilled analysis team, made up of people from different levels as well as departments, gather input from the their organization, analyze the results and act upon them in a structured and methodical manner. This process is effectively aided by the use of the Catalog of Practices, which is, according to Stonebrunner, Gary, Alice and Alexis[17], similar in concept to some of the expert knowledge provided with COBRA.

- ***FRAP***

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. FRAP, as described by Peltier, fully situates itself in the qualitative camp and basically conforms to the standard pattern of risk assessment for qualitative risk. The book titled Information Security Risk Analysis introduced FRAP as the least costly method. Several firms, including RSA – a prestigious organization in information security, have taught the FRAP method for their customers (, URL:http://www.peltierassociates.com/frap.htm[45]).

- ***SPRINT and SARA***

The Information Security Forum (ISF) is a non-profit organization that, in its earlier incarnations, was formed to assess network and computer security on behalf of the European Commission (EC). Today, ISF is an international organization that creates standards and performs research on behalf of its members who fund it. Since the standards and information from ISF are only accessed by its members, information about these methodologies (SPRINT and SARA) is not mentioned here. Briefly, SPRINT is a Simplified Process for Risk IdeNTification. This methodology follows the previously-provided template for risk assessments very closely. SARA, Simple to Apply Risk Analysis for information systems, is supposed to provide more rigor than SPRINT because of efforts that have been determined to involve more complexity or risk (URL:http://www.securityforum.org/ReportsLibrary2002/categories/cat/risk.htm[46]).

4. THE OCTAVE[SM] APPROACH

The first step in managing risk is to understand what our risks are in relation to our organization's mission and its key assets. A comprehensive risk evaluation or assessment can help identify many of the risks. Once they are identified, personnel can put together plans to reduce the risks that are likely to have the highest impact on the organization's assets.

According to Christopher and Audrey[8], current approaches to information security risk management tend to be incomplete. Those approaches are attributed to failing to include all components of risk (i.e. assets, threats, and vulnerabilities). What's worth mentioning is that the organization has insufficient data to fully match a protection strategy to its security risks.

Being sprung from such a thorough observation, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE[SM]) defines the essential components of a comprehensive, systematic, context-driven information security risk evaluation. By following the OCTAVE[SM] method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets. The operational or business units and the IT department work together to address the information security needs of the enterprise.

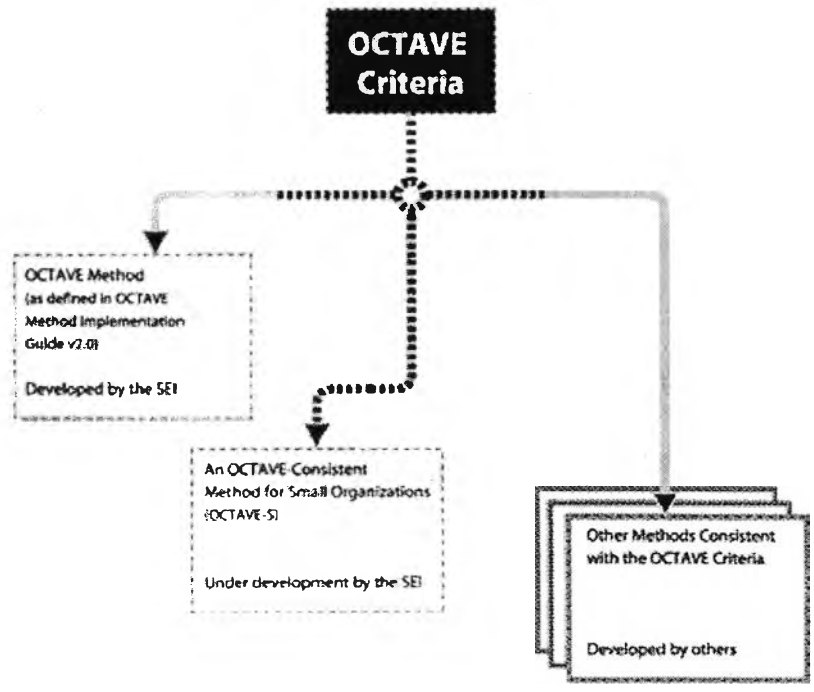

FIGURE 2-4: *The OCTAVE[SM] Approach (URL:http://www.cert.org/octave[37]:*

4.1 Rationale for Selection of This Method

There are nine reasons for selecting the OCATVE[SM] approach:

- The method is developed by CERT/CC (Computer Emergency Response Team/Coordination Center) - a federally funded research and development center – of the Software Engineering Institute (SEI) at Carnegie Mellon University. So far, this 15-year-old center has been a typical model for research and development in the field of computer and network security throughout the world. For example, ThaiCERT (a division of NECTEC, located at the science park), JPCERT/CC (Japan), AUSCERT (Australia), SingCERT (Singapore), SKCERT (South Korea), DFN-CERT (Germany) etc., to name but a few, are mostly adapted from this initial model. Moreover, many prestigious academics and practitioners (i.e. US's National Institute of Standard and Technology - NIST, US's Computer Security Institute – CSI, etc.), when writing their publications, all cite CERT's work to clarify their points.

- As far as I have studied, many of the current models are 'bottom-up': They start with the computing infrastructure and focus on the technological vulnerabilities without considering the risks to the organization's mission and business objectives. Instead, according to Christopher and Audrey[8], a comprehensive information security risk evaluation approach should:
    - Incorporate asset, threat and vulnerabilities;
    - Enable decision-makers including non-technical to develop relative priorities based on what is critical to their organization;
    - Incorporate organizational issues related to how people use the computing facilities to meet the business objectives of the organization. This idea will be discussed more in regard to the asset-driven evaluation approach;
    - Incorporate technological issues related to the configuration of the computing facilities;
    - Be a flexible method that can be uniquely tailored to each organization

  The OCATVE[SM] method was born in accordance with those ideas. Thus, it is different from typical technology-focused assessments since it focuses on organizational risk and strategic, practice-related issues, balancing operational risk, security practices, and technology.

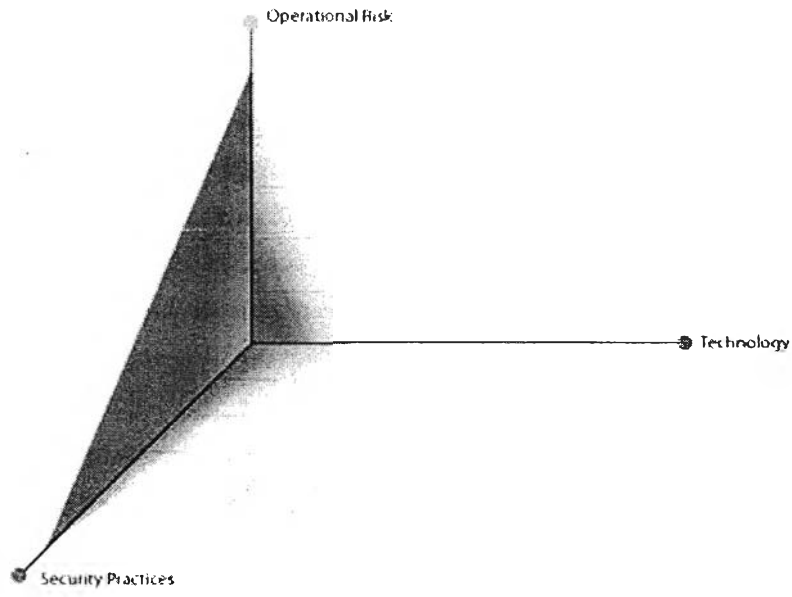

FIGURE 2-5: *OCTAVE[SM] balances operational risk, security practices, and technology*
Source: *URL:http:www.cert.org/octave/*[37]

As the figure illustrates, the OCTAVE approach is driven by operational risk and security practices. Technology is examined only in relation to security practices.

- OCTAVE[SM] is an asset-driven evaluation approach, framing the organization's risks in the context of its assets. Therefore, according to Fites, Kratz and Brener[24], using the organization's assets to focus the evaluation's activities is an efficient means of reducing the number of threats and risks that we must consider during the evaluation.

- OCTAVE[SM] is a qualitative approach, which has been analyzed above as a properly and conveniently-implemented way for IT. Similarly, a technique, namely scenario planning is adopted to reflect the nature of IT problem – lack of condition for full observation as well as the dizzy changes of IT.

- OCTAVE[SM] designs a basic set of criteria for the evaluation and then develop a series or family of method meeting those criteria. It stands to this design that this approach is self-directed or self-driven. As such, organizations are able to tailor the approach to suit their specific context and carry out in their own way provided that the above-mentioned criteria are not broken.

- In effect, many organizations outsource information security risk evaluations, which can have drawbacks (Christopher and Audrey[8]). There are, two reasons claimed for these: (1) The organization has no way to know whether the risk assessment performed is adequate for their enterprise (2) It is also impossible for external experts to assume the perspectives of the organization. Therefore, I believe that self-directed assessments provide the context to understand the risks and to make informed decisions and tradeoffs when developing a protection strategy.

- OCTAVE[SM] focuses on practice-based mitigation using recognized, good security practices. For instance, the BS 7799:1995 is among important sources to create the catalog. This characteristic, in my opinion, brings us two distinct advantages. Using best practices as a benchmark to compare with current organizational practices is both realistic and effective since it helps organizations to quickly realize what are their strengths and weaknesses without confusing. Next, best practices partly based on British Standards is quite convenient because of the compatibility with the ISO 17799:2000.

- OCTAVE[SM] includes staff from business and IT department at all level. This characteristic, in my opinion, helps consider the organization from different perspectives.

- Last but not least, OCTAVE[SM] is an elaborate, ongoing project (whilst other methods were a kind of one-shot and only created by few people!) performed by a diversified group of many experts on business and security. It's promising that more effective enhancements will be added to the approach so that it serves well the purpose of organizations.

4.2 The Octave[SM] Methodology

The journey of understanding about information security risk evaluations begins with the fundamentals, which include principles, attributes and outputs of the OCTAVE[SM] approach. Grasping such important characteristics of the OCTAVE[SM] will be useful since it lays the foundation for specific implementations. But first, I'll come up with what is the structure of the OCTAVE[SM].

4.2.1 The OCTAVE[SM] Structure

Using a three-phase approach, OCTAVE[SM] examines organizational and technology issues to assemble a comprehensive picture of the information security needs of an enterprise. The phases of OCTAVE[SM] are:

- **Phase 1: Build Asset-Based Threat Profiles** - This is an organizational evaluation. Key areas of expertise within the organization are examined to identify important information assets, the threats to those assets, the security requirements of the assets, what the organization is currently doing to protect its information assets (protection strategy practices), and weaknesses in organizational policies and practice (organizational vulnerabilities).

- **Phase 2: Identify Infrastructure Vulnerabilities** - This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are examined for weaknesses (technological vulnerabilities) that can lead to unauthorized action.

- **Phase 3: Develop Security Strategy and Plans** - Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) are analyzed to identify risks to the enterprise and to evaluate the risks based on their impact to the organization's mission. Lastly, a protection strategy for the organization and mitigation plans addressing the highest priority risks are developed.

Perhaps, the first impression comes to the readers, when considering the formal OCTAVE[SM] approach, is that it comprises of a progressive series of workshops, each of which requires interaction among its participants. More concretely, it is broken into eight processes: four in phase 1, two in phase 2 and two in phase 3.

The diagram below provides the readers with a panorama of the approach:

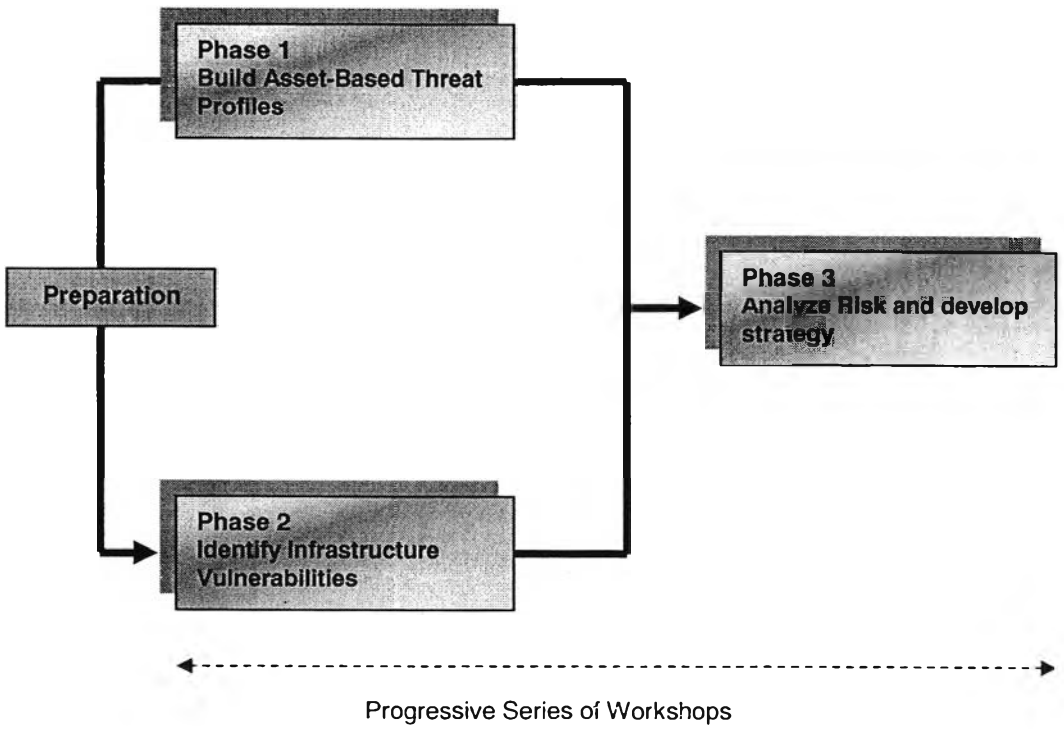

FIGURE 2-5: *The 3 phases and contents of OCTAVE[SM] Approach*
Adapted from Figure 3-1, p.44, Christopher and Audrey[8]

➢ ***Phase 1: Build Asset Threat Profile (Processes 1 to 4)***

Phase 1 begins with the organizational view of OCTAVE[SM] by focusing on the people in the organization. Figure 2-6 illustrates the four processes conducted in phase 1.

I21601719

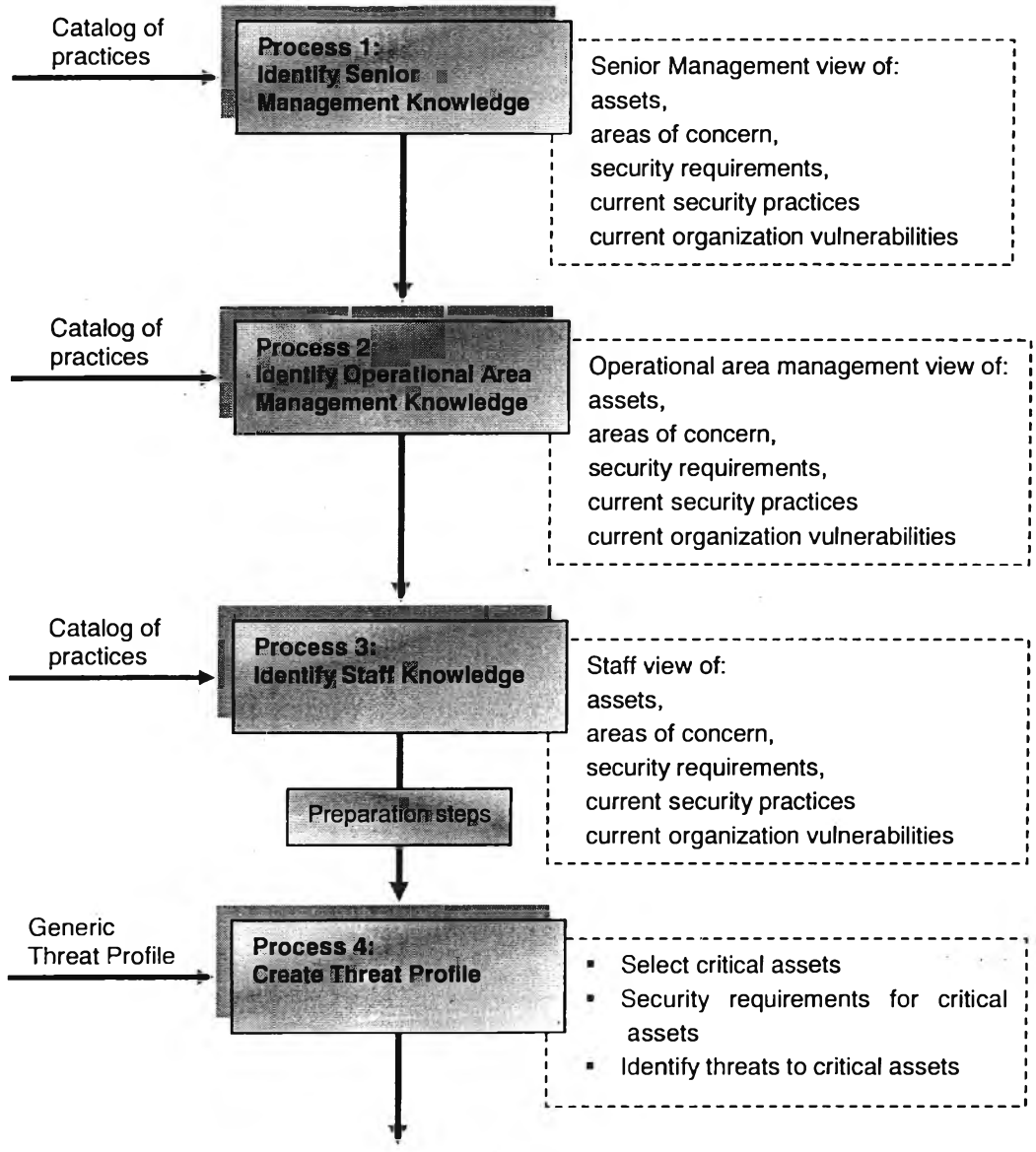

FIGURE 2-6: *Phase 1: Build Asset-Based Threat Profiles*

➢ ***Phase 2: Identify Infrastructure Vulnerabilities (Processes 5, 6)***

Phase 2 is also named the 'technological view' of the OCTAVE[SM] Method since there is a turning of attention from 'organizational view' in Phase 1 to 'technological view'. As mentioned in the previous sections, this phase always comes first in many risk evaluation of information professional, which reveals the weakness due to sticking too much to technological issues. The participants are the analysis team and selected members of the IT staff.

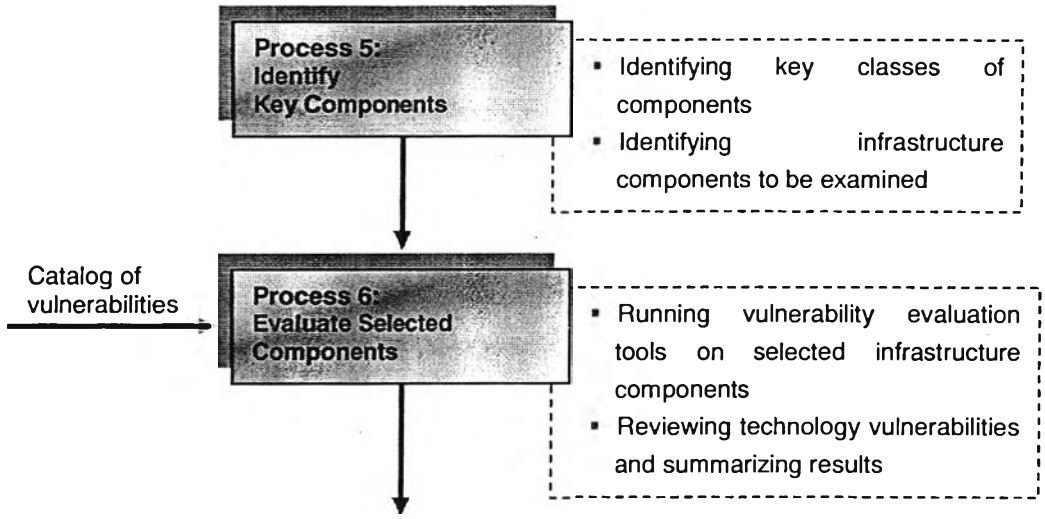

FIGURE 2-7: *Phase 2: Identify Technological Vulnerabilities*

➢ ***Phase 3: Conduct Risk Analysis (Process 7,8)***

Phase 3 is designed to make sense of the information that we have gathered so far in the evaluation. The phase is closed with developing protection strategy and plans.

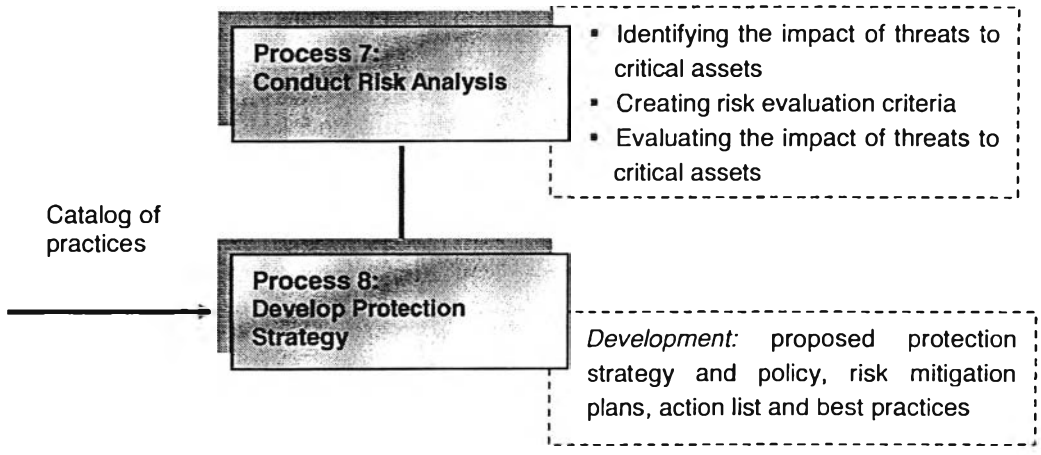

FIGURE 2-8: *Phase 3: Conduct Risk Analysis*

After reviewing the OCTAVE[SM] approach, readers would probably have an idea of how the OCTAVE[SM] is structured as well as which task to be conducted in each process.

As I mentioned in section 5.1, one of the most impressive points in implementing the OCTAVE[SM] is that it is designed with the thought in mind that a 'one-size-fits-all' doesn't work for evaluating information security risks. Different organizations differing in size may develop different ways to conduct the method so long as they stick to the set of criteria defined by OCATVE[SM]. Thanks to this interesting characteristic, I'll tailor the above-presented approach to fit the context of the case study.

4.2.2 The OCTAVE[SM] Principles & Attributes

Here come the philosophical underpinnings of an information security risk management approach. The principles shape the nature of risk management activities and provide the basis for the evaluation process. OCTAVE[SM] groups principles into the following areas:

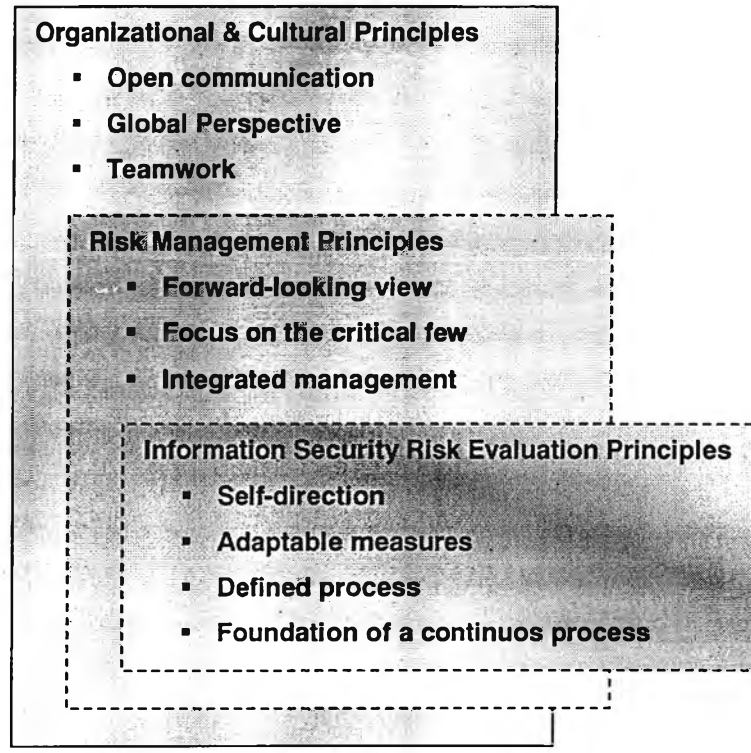

FIGURE 2-9: *Information Security Risk Management Principles Adapted from Figure 2-1, Christopher and Audrey[8] (2003).*

➢ ***Information Security Risk Evaluation Principle***

These principles are important concepts that drive the information risk evaluation principles.

- ***Self-Direction***

The OCTAVE[SM] method is self-directed. A small team of the organization's personnel (called the analysis team) manages the process and analyzes all information. Thus, the organization's personnel are actively involved in the decision-making process. To be specific, self-direction requires:

- Taking responsibility for information security by leading the information security risk evaluation and managing the evaluation process
- Making the final decisions about the organization's security efforts, including which improvements and actions to implement

- ***Adaptable measures***

A flexible evaluation process can adapt to changing technology and advancements. It is not constrained by a rigid model of current sources of threats or by which practices are currently accepted as 'best'. This, in my opinion, is essential when considering the impressive evolution of IT in recent years. Adaptable measures require:

- Current catalog of information that define accepted security practices, known sources of threat and known technological weakness (vulnerabilities)
- An evaluation process that can accommodate changes to the catalogs of information

- ***Defined process***

It is crucial for information security evaluation programs to rely upon defined and standardized evaluation procedures Using a defined evaluation process helps to institutionalize the process, thereby ensuring some level of consistency in the application of the evaluation. A defined process requires:

- Assigning responsibilities for conducting the evaluation
- Defining all evaluation activities
- Specifying all tools, worksheets and catalogs of information required by the evaluation
- Creating a common format for documenting the evaluation results

- ***Foundation of a continuous process***

An organization should implement practice-based security strategies and plans to improve its security posture over time. Doing so, an organization can institutionalize good security practices, making them part of the way the organization routinely conduct business. The results of an information security risk evaluation provide the foundation for continuos improvement, which requires:

- Identifying information security risks using a defined evaluation process
- Implementing the results of information security risk evaluation
- Setting up the ability to manage information security risks over time
- Implementing security strategies and plans that incorporate a practice-based approach to security improvement

➢ ***Risk Management Principles***

Risk management underpins with the following principles:

- ***Forward-looking review***

A forward-looking review requires an organization's personnel to look beyond the current problems by focusing on risks to the organization's most critical assets. The focus is on managing uncertainty by exploring the interrelationship among assets, threats and vulnerabilities and examining the resulting impact on the organization's mission and business objectives. This principle requires thinking about tomorrow, focusing on managing the uncertainty presented by a range of risks. Additionally, it requires managing organizational resources and activities by incorporating the uncertainty presented by information security risks.

- ***Focus on the critical few***

This principle requires the organization to focus on the most critical information security issues. Understandably, every organization faces constraints on the number of staff members and funding that can be used for information security activities. Thus, the organization should ensure that it is applying its resources effectively during and after the evaluation. This principle requires:

- Using targeted data collection to collect information about security risks
- Identifying the organization's most critical assets and selecting security practices to protect those assets

- ***Integrated management***

This principle requires that security policies and strategies be consistent with organizational policies and strategies. The organization's management proactively considers trade-offs among business and security issues when creating policy, striking a balance between business and security goals. Integrated management means:

- Incorporating information security issues into the organization's business processes
- Considering business strategies and goals when creating and revising information security strategies and policies

➢ ***Organizational & Cultural Principles***

These principles help to create an organizational culture conducive to effective risk management. Without such a culture, people may not communicate or work together to address risk issues.

- ***Open communication***

The principle, considered to be the most important of the OCTAVE[SM], is also the most difficult to implement. A fundamental concept behind most successful risk management program is a culture that supports open communication of risk information through a collaborative evaluation approach. For instance:

- Developing evaluation activities that are built upon collaborative approaches (e.g. workshops)
- Encouraging exchanges of security and risk information among all levels of an organization
- Using consensus-based processes that value the individual voice.

- ***Global perspective***

This principle requires the members of the organization to create a common view of what is most important to the organization. This means:

- Identifying the multiple perspectives of information security risk that exist in the organization
- Viewing information security risk within the larger context of the organization's mission and business objectives

This principle, in my opinion, is tough to implement to large, complex organization since it requires those who provide common view should have a strategic view of the organization at a macro level.

- ***Teamwork***

Hardly an individual can understand all of the information security issues facing an organization. This explains why OCTAVE[SM] puts much emphasis on interdisciplinary approach, including both personnel from IT and business department:

- Creating an interdisciplinary team to lead the evaluation
- Knowing when to include additional perspectives in the evaluation activities
- Working cooperatively to complete evaluation activities
- Leveraging people's talents, skills and knowledge

Readers may simply understand the above-presented principles as 'viewpoints' of the OCTAVE[SM] method and wonder what'll make such 'viewpoints' come into existence. In other words, what strategy and tools or techniques will be adopted to transform those 'points of view' into action. The answer lies in the mapping from principles into attributes below.

Principles	Attributes
Self-direction	Analysis team
	Augmenting analysis team skills
Adaptable measures	Catalog of practices
	Generic threat profile
	Catalog of vulnerabilities
Defined process	Defined evaluation activities
	Documented evaluation results
	Evaluation scope
Foundation for a continuos process	Next step
	Catalog of practices
	Senior management participation
Forward-looking view	Focus on risk
Focus on the critical few	Evaluation scope
	Focused activities
Integrated management	Organizational and technological issues
	Business and information technology participation
	Senior management participation
Open communication	Collaborative approach
Global perspective	Organizational and technological issues
	Business and information technology participation
Teamwork	Analysis team
	Augment analysis team skills
	Business and information technology participation
	Collaborative approach

TABLE 2-1: *Mapping OCTAVE[SM] Principles to Attributes.*
Adapted from TABLE 2-2, p.26, Christopher and Dorofee[8].

- ***Analysis Team***

OCTAVE[SM] requires an analysis team to conduct the evaluation and to analyze the information. The analysis team is an interdisciplinary team comprising representatives from both business and information technology areas of the organization. This attribute is considered important because it ensures that ultimate responsibility for conducting the evaluation is assigned to a team of individuals from the organization. Typically, the analysis team will contain about three to five people, depending on the size of the overall organization and the scope of the evaluation. The basic tasks of the analysis team are to

- facilitate the knowledge elicitation workshops of Phase 1
- gather any supporting data that are necessary
- analyze threat and risk information
- develop a protection strategy and policy for the organization
- develop mitigation plans to address the risks to the organization's critical assets

Thus, the analysis team must have knowledge of the organization and its business processes (including mission-related processes and information technology processes), facilitation skills and good communications skills.

- ***Augmenting analysis team skills***

It is noteworthy that the analysis team is the core team for analyzing information and for making decisions. The core members of the analysis team may not have all of the knowledge and skills needed during the evaluation. At each point in the process, the analysis team members must decide if they need to augment their knowledge and skills for a specific task. They can do so by including others in the organization or by using external experts. For example, when they are analyzing data from a vulnerability tool, the analysis team members might want to invite a member of the organization who has vast information technology knowledge.

- ***Catalogs of Information***

OCTAVE relies upon the following major catalogs of information:

- *Catalog of practices* - a collection of good strategic and operational security practices. Practices in this catalog were derived from CERT/CC, British Standard Institute, the National Institute for Standard and Technology (NIST) and US government regulations. In near future, considering the Thai context, I would suggest that the catalog of practice should be

established as a result of common work of ThaiCERT, Thai Industrial Standard Institute (TISI) and Thai royal government regulation.

- *Threat profile* - the range of threats that an organization needs to consider
- *Catalog of vulnerabilities* - a collection of vulnerabilities based on platform and application

An organization that is conducting OCTAVE[SM] benchmarks itself against the above catalogs of information. During Phase 1, the organization uses *the catalog of practices* as a benchmark for what it is currently doing well with respect to security (protection strategy practices currently being used) as well as what it is not doing well (organizational vulnerabilities). The analysis team may also rely on the *catalog of practices* when preparing controls of risks for ISMS (See Appendix A-0). If an organization must comply with a specific standard of due care, the catalog of practices can be tailored to that standard. The organization then uses *the tailored catalog of practices* as its benchmark for information security readiness, allowing them to understand their security practices in relation to their industrial standard.

After the analysis team selects the critical assets for the organization, they use *the Threat Profile,* whose a broad range of known potential threat sources is formally defined, to create the range of threat scenarios that affects each critical asset. This occurs in process 4 (the end of Phase 1).

The analysis team uses vulnerability evaluation tools (i.e. software, checklists, scripts), which are either freeware or commercial, to examine their computing infrastructure for weaknesses (technology vulnerabilities) in process 6 (end of Phase 2). Those vulnerability evaluation tools incorporate a *catalog of vulnerabilities* to check the organization's systems, components and devices for technology-based weaknesses. Two examples of catalogs of vulnerabilities are CERT® Knowledgebase (URL:http://www.cert.org/kb[37]) and Common Vulnerabilities and Exploits (CVE - URL:http://www.cve.mitre.org[47]). OCTAVE[SM] does not require specialized software tools for the technology vulnerability evaluation.

- ***Defined evaluation activities***

The procedures for performing each evaluation activity and the artifacts (i.e. worksheets, catalogs, etc.) used during each activity should be defined and documented:

- Procedures for preparing the evaluation
- Procedures for scoping the evaluation
- Procedures for completing each evaluation activity
- Specifications for all tools and worksheets required by each activity
- Specifications for catalogs of information that define accepted security practices, known sources of threat and known technological weaknesses

Implementing defined evaluation activities helps to institutionalize the evaluation process in the organization, ensuring some level of consistency in the application process (US GAO[25]).

- ***Documented evaluation results***

The organization should document the results of the evaluation, either in paper or electronic form. It is important to establish a permanent record of evaluation results (database), which can serve as source material for subsequent evaluations and can be useful when tracking the status of plans and policies after the evaluation. Let's say, if risks to a critical asset are identified, staff members can look at the threat profiles of risks to similar assets. Personnel can then understand which risks were mitigated effectively in the past and which were not. Furthermore, I would think that this principle is suitable to one of important requirements for establishing ISMS in this study (which will be presented in Section 4.4 of Chapter 3) – documenting risk assessment results and conclusion.

- ***Evaluation scope***

The extent of each evaluation must be defined. The evaluation process should include guidelines to help the organization decide which operational areas to mention in the evaluation. Setting a manageable scope for the evaluation reduces the amount of work of the evaluation. In addition, the areas of an organization can be prioritized for the evaluation.

- ***Next step***

The evaluation should include an activity whereby personnel identify the next steps required to implement security strategies and policies. This often requires

active sponsorship and participation from the organization's senior management. This attribute is essential for security improvement. For example, after OCATVE[SM] there should be a statement on applying strategy and policy to mitigate the identified risks. Like the principle of documented evaluation results, this also fits one of requirements for establishment of ISMS – Statement of applicability (which will be presented in Section 4.4 of Chapter 3).

- ***Focus on risk***

Examining the interrelationship among assets, threats to the assets and vulnerabilities including both the organizational and technological weaknesses is a must. Staff members should look beyond the current organizational and technological weaknesses and examine how those weaknesses relate to the organization's critical assets accompanied by the effect on the organization's business objectives and mission.

- ***Focused activities***

The evaluation process should include guidelines for focusing evaluation activities:

- Workshops that efficiently elicit security-related information from an organization's staff members. For example, in processes 1 to 3, team focuses the activities on the assets believed to be the most critical.
- Analysis activities that use asset information to focus threat and risk identification activities. For example, in process 4, team focuses its activities on using the selected assets.
- Analysis activities that use asset and threat information to set the scope of the technology vulnerability evaluation. For example, in processes 5 and 6, team sets the scope of the infrastructure vulnerability evaluation using the organization's critical assets and identified threats (e.g. human actors using network access).
- Planning activities that establish risk priorities using risk measures (impact, probability). For example, in processes 7 and 8, team establishes risk priorities based on the organizational impact and probability of risks.

- ***Organizational and technological issues***

The evaluation process must examine both the organizational and technological issues:

- Current effective security practices used by staff members.
- Missing or ineffective security practices (also known as organizational vulnerabilities). Both requirements are obtained at the end of phase 1.
- Technological weaknesses present in key information technology systems and components. This is obtained at the end of phase 2.

The organizational and technological data are then analyzed during phase 3. Thus, the analysis team is able to address security by creating a global picture of the information security risks.

- ***Business and information technology participation***

The evaluation process must include participants from both the business and information technology departments, allowing for the establishment of an interdisciplinary analysis team (see the analysis team attribute). Furthermore, participants must include representatives from multiple organizational levels (i.e. senior management, operational area manager and staff). This attribute ensures that a broad range of risk factors is considered.

- ***Senior management participation***

Senior management demonstrates active sponsorship, participate in the workshops to contribute their understanding of security-related issues (i.e. Processes 1 to 3) and their effect on the business processes (i.e. Process 7, 8), review and approve security plans and steps. The level of sponsorship helps to ensure that staff members are available and willing to participate in the evaluation.

- ***Collaborative approach***

Each activity of the evaluation process must include interaction and collaboration among the participants. Collaboration can be obtained through the use of workshops. This is decisive since security is interdisciplinary in nature, completing the evaluation activities requires interdisciplinary knowledge.

4.2.3 The Outputs of OCTAVE[SM]

Outputs are the results or outcomes that the analysis team must achieve during the evaluation. Basically, there are three types of outputs: (1) organizational data (2) technological data (3) risk analysis.

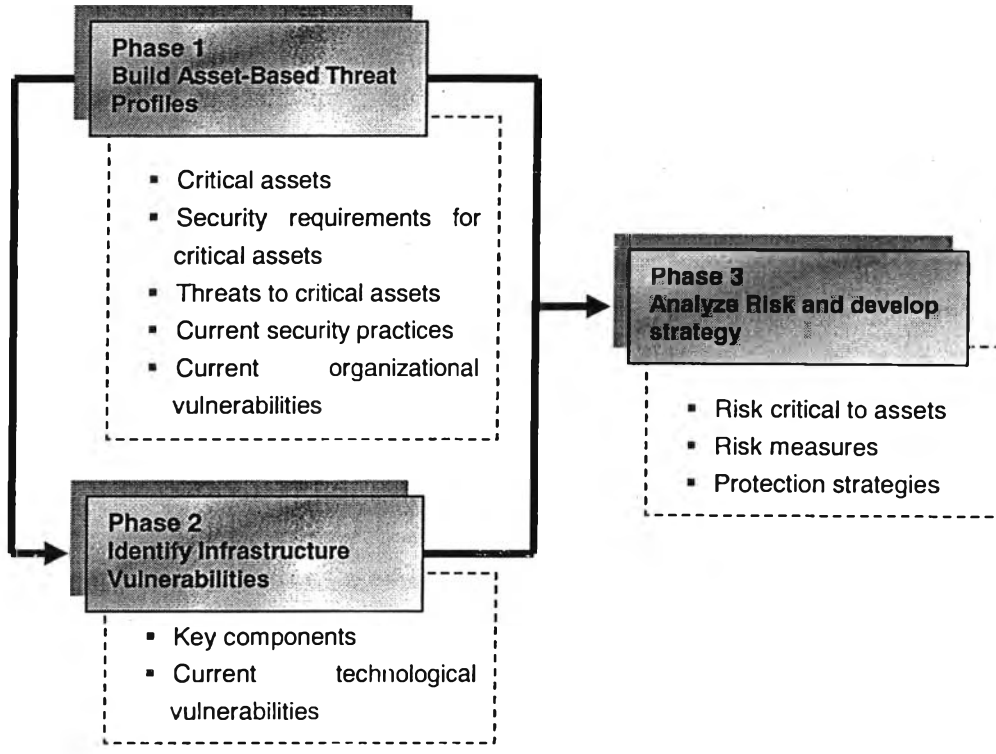

FIGURE 2-11: *OCTAVE[SM] Outputs.*
Adapted from Figure 2-2, p.34, Christopher and Audrey[8].

4.2.4 Preparation for OCTAVE[SM]

Planning for OCTAVE[SM] creates the foundation for a successful evaluation. Here are the key factors:

- ***Getting senior management sponsorship*** – The planning activities for OCTAVE[SM] start with senior management sponsorship. This could require briefings to senior management to help them understand the process. Once understanding, they'll support the process and thus, people tend to actively participate. Otherwise, people will miss workshops and the analysis team will not have the ability to convince people to attend.

- ***Selecting the analysis team*** - Representatives from both the business and information technology parts of the organization will be on the analysis team. The size of the analysis team is three to five people. Senior managers should be involved in the selection of team members. In addition, it is helpful if some of the members come from the operational areas that will be participating in the evaluation.

- ***Scoping OCTAVE^{SM}*** – Operational areas involved in the evaluation will be properly defined so that the evaluation tasks are conveniently carried out.

- ***Selecting participants*** - During the knowledge elicitation workshops (Processes 1 to 3), staff members from multiple organizational levels will contribute their knowledge about the organization. Moreover, people with special skills to augment the analysis team at certain points in the process need to be selected. The analysis team members will lead the selection of participants. They need to get input from the senior managers as well as the managers for each of the operational areas participating in the evaluation.

- ***Train analysis team.*** The analysis team needs to be trained in the OCTAVE^{SM} Method. Each member of the analysis team needs to understand his or her role during each workshop.

- ***Coordinate logistics.*** The analysis team members need to ensure that rooms, equipment (i.e. computer, projector, etc.) and any supporting data are available for all workshops.

- ***Brief all participants.*** The analysis team should conduct a briefing for all participants prior to their participation in the process.

Once the planning is completed, the organization is ready to start the evaluation.

Details on conducting OCTAVE^{SM} will be mentioned in Chapter 4. Readers will see how this method is implemented in a real case study.

5. ASSISSTED-RISK-ASSESSMENT SOFTWARE TOOLS

In this study, risk assessment is carried out manually. In effect, for large-scale, dispersed organizations, it is required a computer-aided-risk-assessment (CARS) to perform due to a large amount of work. Currently, there are numerous CARS written by risk consulting and analysis companies throughout the world. The risk models adopted are quite different. Some use quantitative approach or qualitative or combination of both. It's suggested that organizations should select those, which suit their specific context and budget.

Below is the list of CARSs that mostly perform from an information security perspective. Information on these products is collected during the time of this study – 2003 and 2004.

CARS Name	Producer
APT Open System Tools	APT ltd. 3rd Floor State Street New York, NY 10004, USA URL:http://www.apt.com/en/products/software.html
CORA	International Security Technology, Inc 99 Park Avenue, 11th Floor, New York, NY 10016-1501, USA Telephone:+1(212)557-0900 FAX: +1 (212) 808-5206 URL:http://www.ist-usa.com/aboutcora.htm
CRAMM	BIS Applied System Limited Stephenson House 75 Hampstead Road London NW1 2PL Tel: +44 20 7637 9111 Fax: +44 20 7468 7006 Great Britain URL:http://www.logicacmg.com/
VaRworks® | MakeVC®	Financial Engineering Associates 2484 Shattuck Avenue, Suite 225 Berkley, CA 94704-20-29, USA Telephone: +1-510-548-6200 Fax: +1-510-548-0332 URL:http://www.fea.com/products/
HAZOP/SVA-Pro™	AcuTech Consulting, Inc. 1948 Sutter Street San Francisco, CA 94115, USA Telephone: (415) 772-5972 Fax: (415) 772-5975 URL:http://www.acutech-consulting.com

CARS Name	Producer
INTEX	Intex Solutions, Inc. 110 A Street Needham MA 02494 USA Telephone: 781 449 6222 Fax: 781 444 2318 URL:http://www.intex.com
RICOS	Algorytmisc 185 Spadina Avenue Toronto, Ontario M5T 2C6 Canada Telephone: 1-416-217-1500 Fax: 1-416-971-6100 URL:http://www.algorithmics.com
Foundstone Enterprise Risk Solution (ERS)	Foundstone Enterprise™ URL:http://www.foundstone.com/index.htm?subnav=products/navigation.htm&subcontent=/products/overview.htm

TABLE 2-2: *CARS products*

6. CONCLUSION

Thomas Finne[26] suggested three rules for dealing with risk. This can, in my opinion, be of great help to all organizations attempting to mitigate the risks:

- Do not take bigger risk than you afford to lose;
- Do not take big risk for small profit;
- Think about possible losses.

Performing risk analysis plays a key role in developing an information security management system. It helps organizations identify the weaknesses in terms of organization and technology vulnerabilities and put the organizations in an active position to face with risks effectively. Hardly can we build a house on a ground without knowing anything about what is beneath the house's foundation. Thing holds true in the area of IT.

The immediate advantages to an organization from application of information security risk analysis and assessment methods include identification of the organization's important assets, potential threats against these assets, security requirements for these assets, and weaknesses or vulnerabilities in current practice that increase the likelihood of these assets being compromised. Armed with this understanding, senior management and information professionals can make reasonable decisions focusing attention on priority assets.

May I quote Chapman's[27] words to end this presentation: "There is a distinction between good luck and good management". Indeed, this is the point that organizations must bear in mind and that threats and risks are not merely the problem of bad luck.

An effective, active preparation of information security is a good solution for dealing with every risk today, as always.