CHAPTER 4

ISMS – A CASE STUDY OF ECC

This chapter materializes the theoretical background introduced and analyzed in chapter 2 and chapter 3. Issues, procedures, tools and techniques will be applied to a specific context – the Engineering Computer Center (ECC). It aims at:

- Conducting the selected Risk Assessment method - OCTAVE[SM].
- Establishing a complete ISMS.

"IT administrators must look for vulnerabilities throughout the organization, but a cracker has to find only one weak link in the chain".
Cameron Sturdevant[34].

1. ECC PROFILE

1.1 An overview

Engineering Computer Center or ECC is the only computer center that serves for the studying and learning needs of lecturers and students at the Faculty of Engineering, Chulalongkorn University. The center composes of 9 computer rooms, 1 room for servers and networking components (i.e. switches, routers, bridges, etc.), 2 offices all scatteredly located at the first and second floor of the Building 3, Faculty of Engineering.

Besides serving the academic activities, the center is also in charge of managing the website of Faculty of Engineering. In the near future, it's expected that the center will be enhanced with visual-audio aided tools and connected with the library of Faculty of Engineering, which will be soon digitized to become a Learning Resource Center (LRC). Once this project is funded and done, the role of ECC will be most important and become a model for other computer centers in the campus.

1.2 Organizational structure

Currently, the center is run by 13 staff members dividing into technical team and administration unit. The function of team:

- Technical team (5 personnel): operates, manages and maintains the computing infrastructure. Moreover, the team must also provide technical support for other offices or divisions of the Faculty of Engineering when necessary.
- Administration unit (6 personnel): operates, manages and protects the whole center. Three personnel are accounting staff.

The organizational structure diagram is as followed:

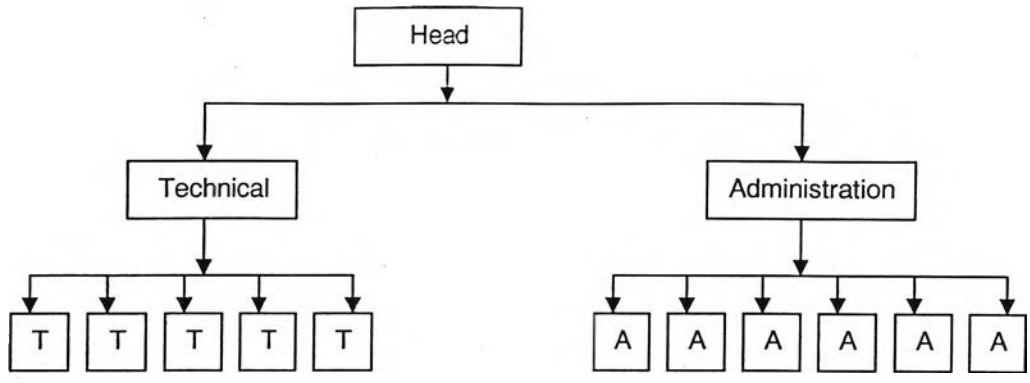

FIGURE 4-1: *ECC's Organizational Structure . Source: ECC.*

1.3 Computing infrastructure

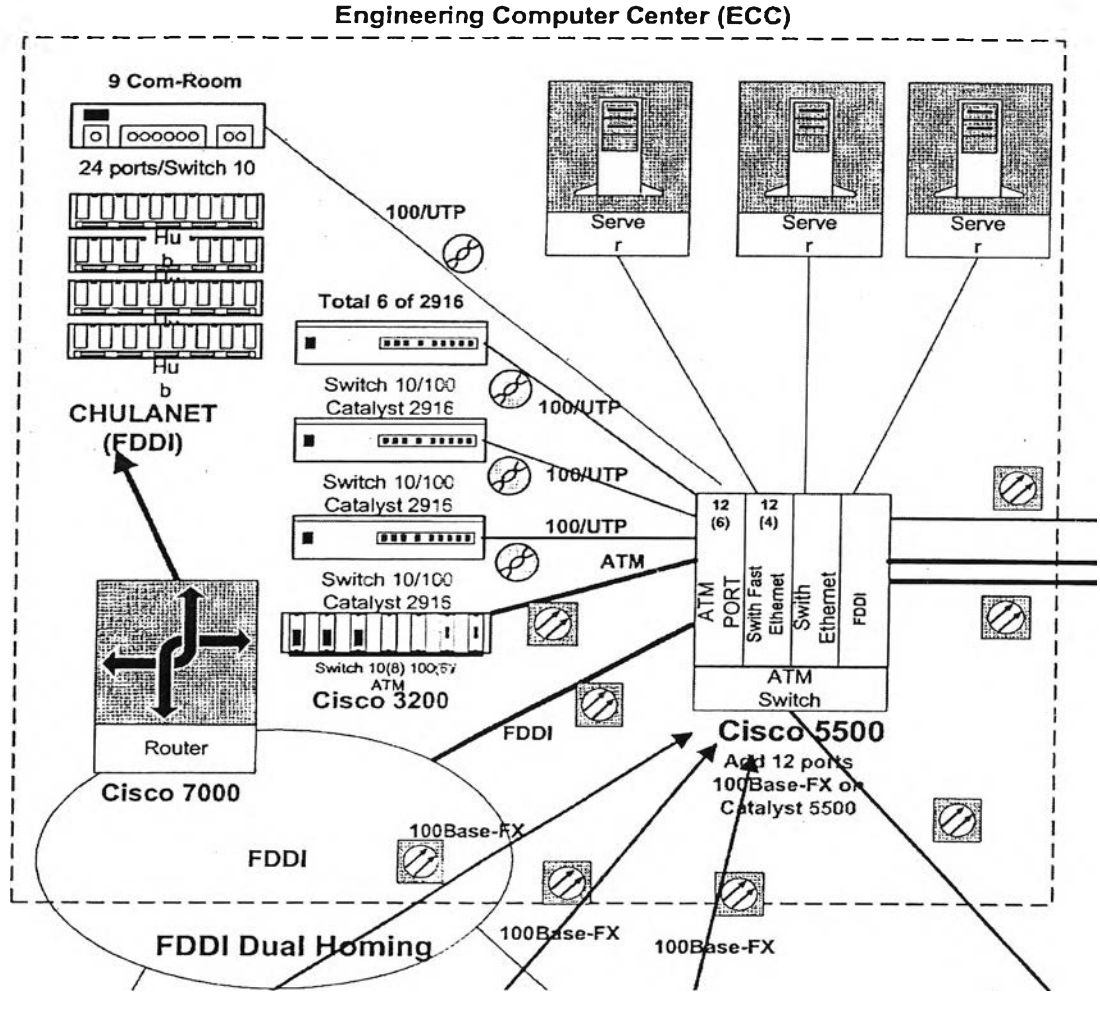

FIGURE 4-2: *ECC's computing infrastructure. Source: Dr.Viboon, ECC.*

At ECC, presently, there are 105 computers in use out of 321 computers, 3 servers, 6 switches, 9 hubs and 1 routers. All computers running on the Windows 2000 operating system and are connected to the CUNET. Besides, there is a Unix center serving for the study of this operating system and other applications on it. ECC's database contains application and programming software, computation data, graphic data, research & learning data, technical data, management data and accounting data.

2. CONDUCTING RISK ASSESSMENT - RESULTS

2.1 Preparation

The OCTAVE[SM] method requires people from both administration unit and technical team to involve in a series of progressive workshops. Due to this nature, a good preparation will be of great help to a successful evaluation.

In Chapter 2, all preparation steps have been thoroughly presented. However, for convenience, I'll highlight some of the key points required for this specific case study.

➢ ***Getting senior management sponsorship for the evaluation***

Sponsorship from senior management is important in terms of:

- Visible, continued support of OCTAVE[SM] activities
- Active encouragement of staff participation
- Delegation of responsibility and authority for accomplishing all OCTAVE[SM] activities
- Commitment to allocate the necessary resources
- Agreement to review the results and make decisions about next steps

➢ ***Selecting the analysis team to lead the evaluation***

The analysis team, as described in Chapter 2, must compose of personnel from both business and IT function, who will be designated by senior management. Since this case study is relatively small, the analysis team includes three members: 1 staff from administration unit, 1 staff from technical team and me. During the progressive workshops, there will be no additional analysis team members.

TABLE 4-1: *Analysis team members*

Member	*Division*
Ms.Anchukorn	Technical
Mr.Thanyawat	Admin
Mr.Keio	Facilitator

The roles and responsibilities of the analysis team include:

- Working with senior management to set the scope of the evaluation, select participants and conducting schedule (Mr.Keio)
- Coordinating with senior management, operational area managers and information technology staff to conduct a vulnerability evaluation for the computing infrastructure
- Gathering, analyzing and maintaining evaluation data during the workshops
- Enabling assessment activities, particularly ensuring that designated personnel attend their specific workshops (Mr.Thanyawat; Ms.Anchukorn)
- Coordinating logistic for the evaluation (Mr.Thanyawat; Ms.Anchukorn)

The core members of the analysis team should possess the following skills:

- Facilitation and good communication skills
- Good analytical skills
- Ability to present to and work with senior management, operational area managers and staff
- Knowledge of the center's business environment
- Knowledge of the center's information technology environment and the admin staff legitimately uses information technology in the center.

➢ ***Setting the scope of the evaluation***

One of the key OCTAVE^{SM} principles is *focus on critical a few*. This means the analysis team can focus their evaluation on selected areas of the center rather than performing an exhaustive search of the entire center. Originally, OCTAVE^{SM} requires choosing at least four areas for consideration. In this case study, the selected operational areas are as followed:

- *Running computing infrastructure for academic activities:* This operational area is selected because it is the mission of the center. The area contains two sub-areas: computing facilities and networking facilities.
- *Managing database system:* The operation of computing facilities results in the needs of storing and processing data regarding users, staff and the center. Thus,

this area contains two sub-areas: managing users' data base, managing staff and the center' database.

Time for conducting this study is approximately two weeks. Since this is a small organization with relatively fat organizational structure, there are two problems to consider: (1) Staff time is very limited (2) Conducting requires a breadth of skills among staff members. To overcome these problems, it's crucial to have a thorough preparation and selection of team analysis members and other participants during progressive workshops.

➢ ***Selecting participants***

The followings are participants in each process to provide information for the analysis team during progressive workshops:

TABLE 4-2: *Participants in each process*

Participants		
Process		*Position*
Phase 1	1,2,3	• Senior management • Two operational area managers from admin unit and technical team • Technical and admin staff
	4	Operational area manager of technical team
Phase 2	5,6	One technical staff + external expert
Phase 3	7,8	Senior management + 1 expert from ThaiCERT

Note: More information on the three phases can be found from pages 36 to 40.

For reading convenience, almost survey results will be put in Appendix A at the very back of the thesis. However, some results and summary, considered necessary for further analysis, will be mentioned throughout section 2.

2.2 Start of Phase 1 – Process 1 to 3

Table 4-3 summarizes the workshop activities for processes 1 to 3. The key activity of processes 1 to 3 is the fourth one, in which participants evaluate the organization's security practices against a catalog of good practices. The results of this activity provide a snapshot of organizational practice and a basis for improvement.

TABLE 4-3: *Processes 1 to 3 activities*

Activity	Description
Identify assets and relative priorities	The participants identify the assets used by the center. They then select the most important assets to the center and discuss their rationale for selecting those assets. Then, for small organization, OCTAVE[SM] allows the analysis team to go farther *by identifying critical assets based on those identified important assets*. On this point, readers may find further information in Section 2.3 below.
Identify areas of concern	The participants identify the scenarios that threaten their most important assets based on typical sources and outcome of threats. They also discuss the potential impact of their scenarios on the center.
Identify security requirements for critical assets	The participants identify the security requirements for their most important assets. In addition, they examine trade-offs among the requirements and select the most important requirement. *Combining with the selected critical assets, the team continues seeking which is the most information security for each critical asset.* Readers may find more explanation in Section 2.3.
Capture knowledge of current organizational security practices and organization vulnerabilities	Participants complete the surveys in which they indicate which practices are currently followed by the center's personnel and which are not. After completing the survey, they discuss specific issues from the survey in more detail.

➢ ***Identify assets and relative priorities***

As I have presented in section 5.1, Chapter 2, OCTAVE[SM] is an asset-driven approach. This is because assets are the main theme of all activities throughout processes 1 to 3. Furthermore, assets guide the selection of devices and components to evaluate technological vulnerabilities in Phase 2. Therefore, it's the intention of my analysis team to gather as much meaningful information as possible.

For definition of assets, readers may find back to section 1.2, Chapter 2. Survey results of this activity can be found at Appendix A-1. Below are the critical information assets identified by participants.

TABLE 4-4: *Critical information assets at the center*

Asset	Description	Rationale
Users' data	Students come and use the computing facilities at ECC. They store their own data for academic purposes	One of the most important objectives of ECC is to provide the students with good facilities for their study. Thus, data stored at ECC must be protected with the highest priority.
Management data	Users' and groups' information (i.e. identification, password, privileges and services), staff's information (i.e. identification, password, privileges and task information), information of ECC's activities with internal and external organizations and ECC's financial and accounting records are digitally stored. All of them form the entire management data.	Without management data, the whole activities at ECC cannot be run. Disclosure, loss or destruction of such information go against the rules as well as regulations of the university.
User Information Processing System (UIPS)	This system helps to manage current user-related data including email system at ECC. Data are monitored and updated on a regular basis and are processed to serve the specific needs of users (i.e. printing, email services and FTP services).	This is also the main objective of ECC. Without the system, ECC's operation will be severely influenced. ECC cannot handle such a large amount of work efficiently.
Personal computers (PCs)	Students utilize PCs for their learning, research and communication.	PCs, along with the above-mentioned users' data, are of the most important to the users' needs.
Network & Networking Components (NCs)	NCs are a means to transmit data within the center and from the center to any other places. It is an indispensable part of the entire CUNET.	Besides PCs, ECC consider NCs as the most important physical asset in daily operation.
Technical team	Technical team is responsible for the operation of ECC in terms of managing, maintaining and developing the computing facilities.	Technical team possesses skills and expertise that ensure a good and stable performance of computing facilities at ECC.

➢ ***Identify areas of concern***

As it can be seen from Figure 2-6, Chapter 2, the purpose of Process 4 is to create asset-based threat profiles in accordance with the threat scenarios described by participants in this step. Known sources of threats and outcomes are used as prompts during participants' brainstorming (See Appendix A-2). Tables A-2.1 and A-2.2 provide readers with some definitions of threat sources and threat outcomes. However, readers may refer to Section 1.3, Chapter 2 for further description of threat outcomes regarding information security requirements for assets.

The summary areas of concern (italic words) for this step are as followed:

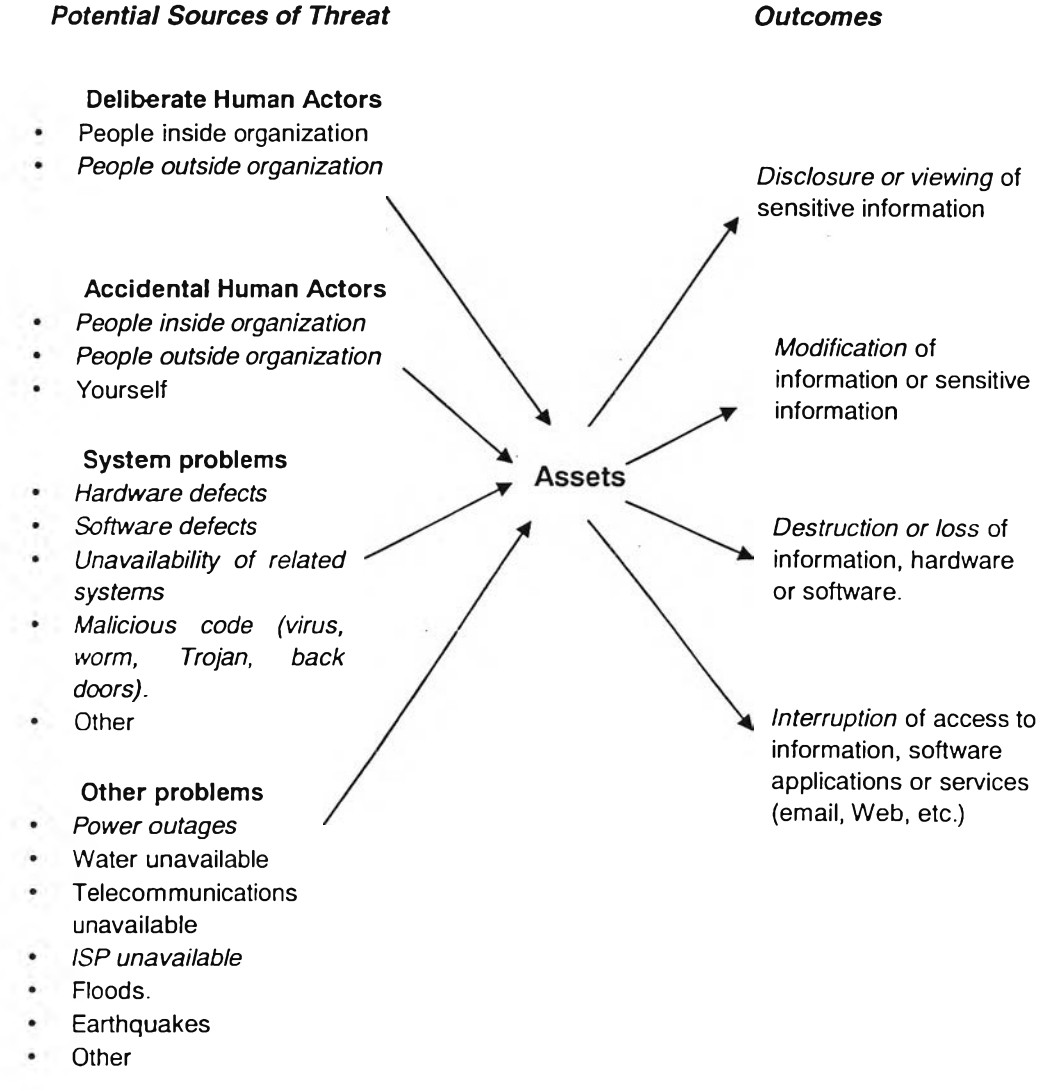

FIGURE 4-3: *Participants identify threat sources and outcomes*
Adapted from p.368, Christopher and Audrey[8].

➢ ***Identify security requirements for most important assets***

To protect critical assets, it's crucial to establish what is important about each of those assets. In this step, participants discuss which qualities are important about the assets that they have identified in previous steps. More specifically, there are two sub-tasks to be taken:

- *Identify security requirements for each critical asset* – In this task, to prompt the participants, the analysis team will provide a small document for participants, whose content is what I have presented in section 1.3, Chapter 2, briefs what are information security requirements as well as examples on each information asset (see Figure 2-3).
- *Prioritize security requirements* – In this task, participants are asked to examine the relative trade-off among the three requirements of each asset.

As I have presented in Table 4-3, in this step, the analysis team also explores which are security requirements for each critical asset and which is the most important security requirement of each critical asset. Survey results of this activity can be found in Appendix A-3.

➢ ***Capture knowledge of current organizational security practices and organizational vulnerabilities***

In order to improve with respect to how the center handles information security, the analysis team needs first to establish where the center currently is, for instance, what they (the center) are currently doing well and where they need to improve. With this thought in mind, the analysis team asks the participants to evaluate their current security practices against a catalog of known good security practices (see Appendix A-0). This catalog of practice is tailored from the original to fit the specific context of ECC – a small organization.

Survey results of this benchmark activity can be found in Appendix A-4.

Since the OCTAVE^{SM} method cannot cover all the information, it thus requires another facilitated discussion about security practices in the organization. Emphasis is put much on organizational vulnerabilities such as weaknesses in organizational policy or practice that can result in unauthorized actions. Details on this task can be found in Appendix A-5.

2.3 Process 4 – End of Phase 1

Process 4 consists of two main activities. The first activity is preparation activity. This is actually a consolidating task, whose purpose is simply to find inconsistencies and gaps among organizational levels by: (1) grouping assets by organizational levels; (2) grouping security requirements by organizational level and asset; (3) grouping areas of concern and impacts by organizational level and asset. For large, complex or dispersed organizations, this step is of utmost importance. However, since the case study is a small organization with a relatively flat organizational structure, there is virtually no gap and inconsistency in terms of surveyed information. OCTAVE[SM] allows the analysis to skip this preparation step. In my opinion, this preparation step can also be done at the end of Process 1 to 3.

As it can be seen from Figure 2-6, there exist three main tasks in the second activity:

- *The first task: Select critical assets* – The analysis team identifies which assets will have a large adverse impact on the center if their security requirements are violated. Those with the greatest impact to the center are the critical assets. OCTAVE[SM] suggests to select at least five. In this case study, my analysis team selected six assets.

- *The second task: Refine security requirements for critical assets* – The analysis team creates or refines the security requirements for the critical assets. Besides, team also selects the most important security requirement for each critical asset. For the first and second tasks, as far as the small organization is concerned, OCTAVE[SM] allows the analysis team to carry out in Process 1 to 3. It means, after collecting data from participants on which assets are important to the center. The analysis team then can do more by identifying which are the critical assets of the center as well as which are the most important security requirement for each critical asset. Readers may turn back to Table 4-3 in Section 2.2 for further information. Details are also provided in each relevant task following the presentation of Table 4-3.

- *The third task: Identify threats to critical assets* – The analysis team identifies the threats to each critical asset by first mapping the areas of concern for each critical asset to a generic threat profile, thereat creating a unique threat profile for that asset. Then, the analysis team also performs a gap analysis to determine additional threats to the critical asset. Since the first two tasks are already done, I'll focus my presentation on this third task.

In order to map areas of concern into a Generic Threat Profile, I find it necessary to introduce the Generic Threat Profile, which is, in my opinion, one of the most effective tools adopted by the OCTAVE[SM] method. It stands to the reason that this Generic Threat Profile is an impressive improvement of the *Ishikawa diagram*, enabling the analysis team to easily and efficiently find the problems (in this method are threats or risk) occurring to the center's assets (*Note:* The authors of OCTAVE[SM] just claimed that this is a tree-based analysis and scenario-based planning). Differing from the original *Ishikawa diagram,* the Threat Profile (of each asset) provides the analysis team with a deep view into the problem, concerning every aspects of a threat to an asset.

In the OCTAVE[SM] method, threats are represented visually in the profile using the following properties:

- *Asset* – something of value to the enterprise
- *Actor* – who or what may violate the security requirements of an asset
- *Motive (or objective)* – whether the actor's intentions are deliberate or accidental (applies only to human actor)
- *Access* – how the asset will be accessed by the actor, e.g. network access, physical access (applies only to human actor)
- *Outcome* – the immediate outcome (disclosure. modification, destruction, loss, interruption) of violating the security requirements of an asset.

Before developing Asset-Based Threat Profiles, I would introduce the Threat Sources. This is widely known types of threats that, according to various experts on information security, might occur to information assets in an organization. It's worth mentioning that, at a glance, Tables A-2.1 and 4-5 appear to be the same. In fact, Tables A-2.1 is only used for eliciting areas of concern from workshop whilst the other is useful for risk analysis.

The Generic Threat Profile is a starting point to create a unique Threat Profile for each critical asset. The analysis team essentially tailors the Generic Threat Profile for each critical asset by deciding which threats in the range of possibilities actually apply to a critical asset. Figure 4-4 to 4-7 present the asset-based threat trees that form the Generic Threat Profile.

TABLE 4-5: Threat Types

Category of Threats	Definition
Human actors using network access	The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
System problems	The threats in this category are problems with an organization's information technology systems. Examples include hardware defects, software defects, unavailability of related enterprise systems, malicious code (e.g. viruses, Trojan horses, etc.) and other system-related problems.
Other problems	The threats in this category are problems or situations beyond the control of an organization. This category of threats includes natural disaster (such as floods, earthquakes and storms) that can effect an organization's information technology systems as well as interdependency risks. Interdependency risks include the unavailability of critical infrastructure (telecommunication, electricity, etc.). Other types of threats beyond an organization's control – power outages, broken water pipes, etc. - can also be included here.

There are a number of ways to tailor the Generic Threat Profile:

- Adding threats in a category
- Including more details threat actor, access, and motive information in the profile
- Deleting threats in a category
- Adding a new threat category
- Deleting a threat category

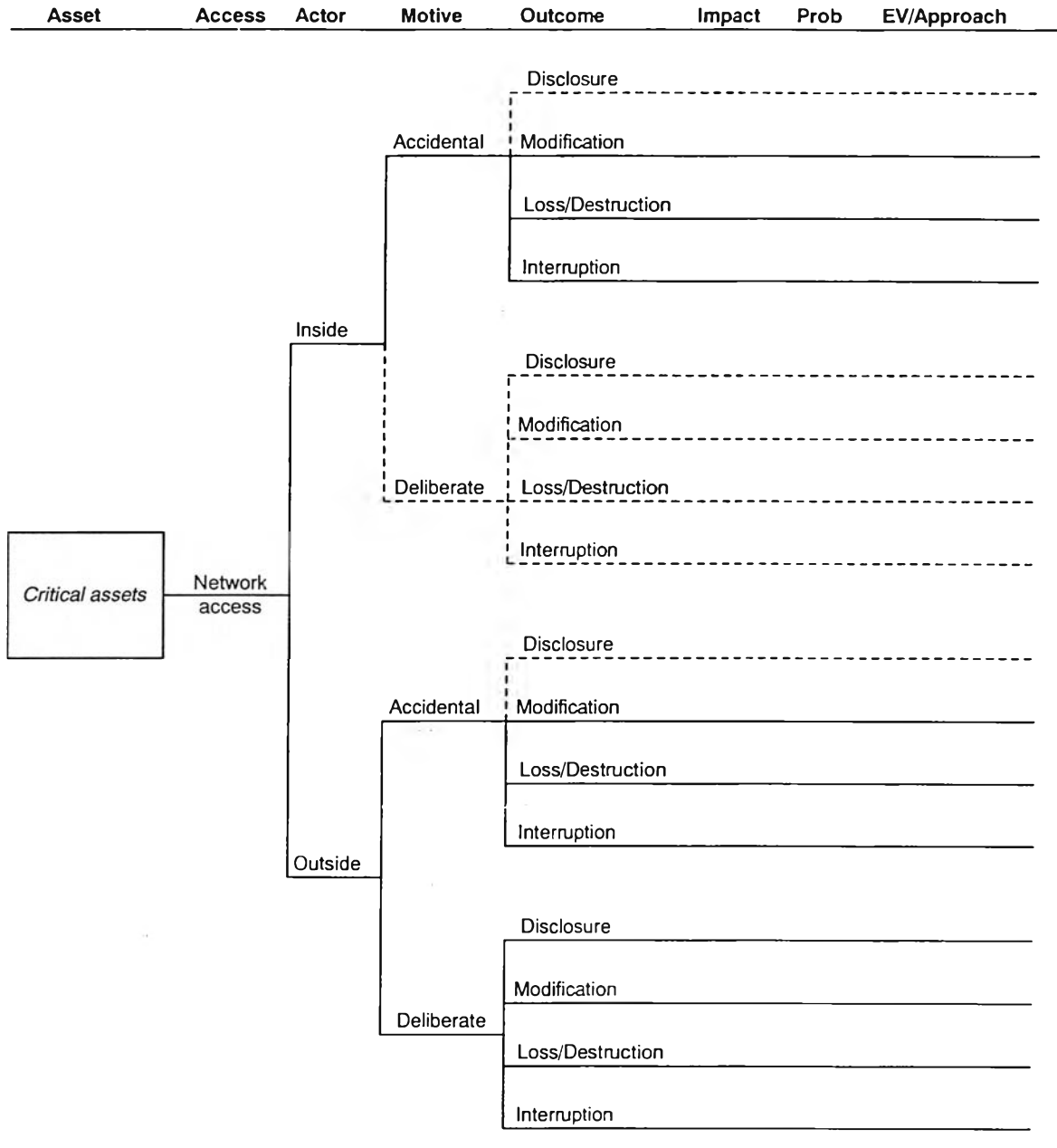

FIGURE 4-4: *Asset-Based Threat Tree for Human Actors Using Network Access.*
Source: *Figure 6-2, p.115, Christopher and Audrey*[8].

Note: *The dashed line represents that no threat exist*

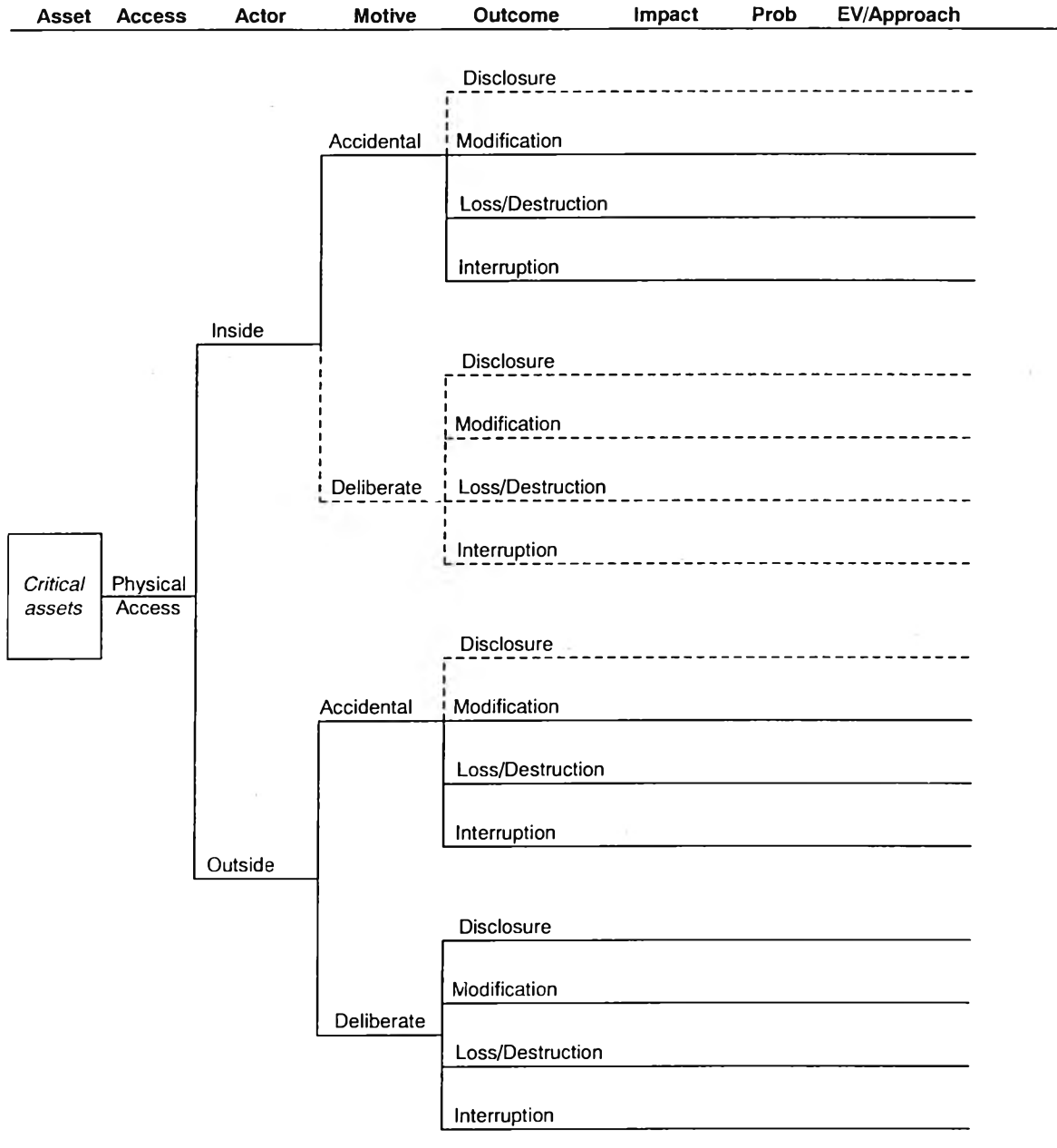

FIGURE 4-5: *Asset-Based Threat Tree for Human Actors Using Physical Access.*

Source: *Figure 6-1, p.114, Christopher and Audrey*[8].

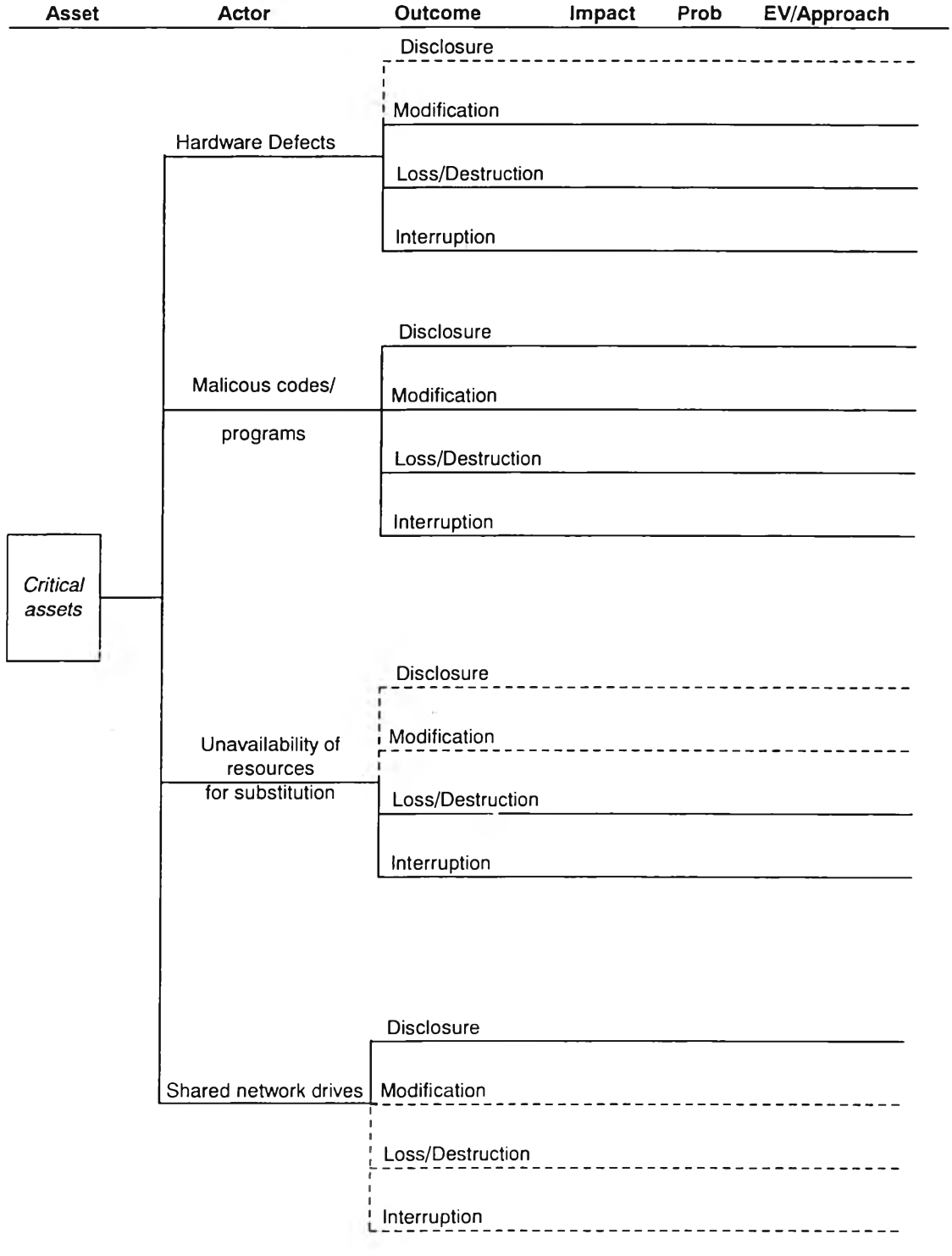

FIGURE 4-6: *Asset-Based Threat Tree for System Problems.*

Source: *Figure 6-3, p.116, Christopher and Audrey[8].*

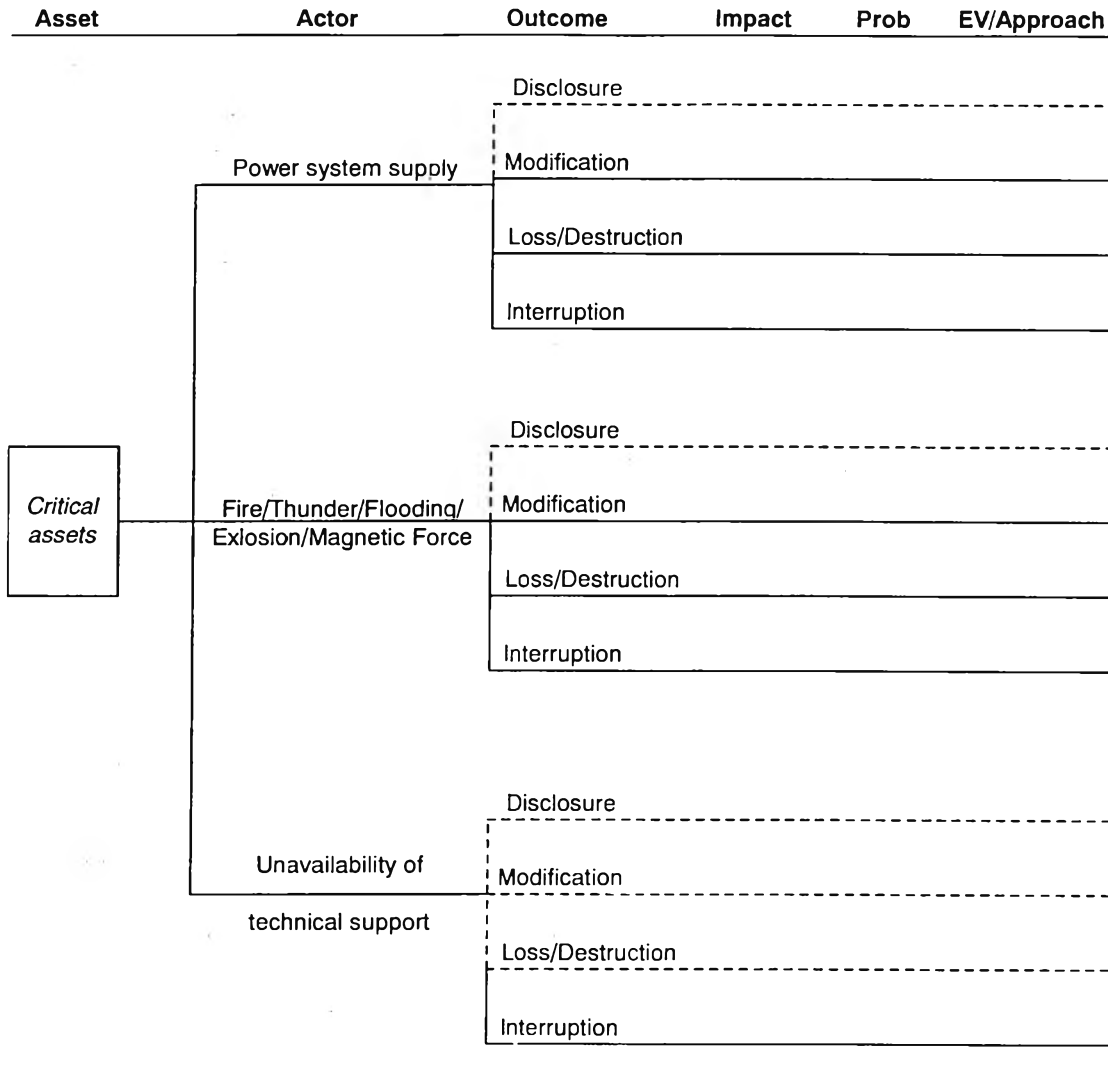

FIGURE 4-7: *Asset-Based Threat Tree for Other Problems.*
Source: *Figure 6-4, p.117, Christopher and Audrey[8].*

After understanding Generic Threat Profile as well as how to tailor it, the analysis team arrives at examining the range of threats that can effect the center's critical assets. OCTAVE[SM] requires three sub-tasks:

- ***Map areas of concern to Generic Threat Profile***

In this sub-task, the team, along with senior management, develops the areas of concern that has been carried out in Process 1 to 3. Areas of concern are now described more specifically and accurately in order to conveniently map into the Threat Profile.

The analysis results obtained can be found in Appendix A-6.

After preparing specific areas of concern, the team draws Asset-Based Threat Profile for each critical asset. However, these are not the final Threat Profiles since there might be a missing of potential threats. This fact results in performing a gap analysis.

➢ ***Perform gap analysis***

In this step, the analysis team tries to determine what other threats could affect the center's critical assets by seeking two questions suggested by OCTAVE[SM]:

- For which remaining potential threats is there a more than negligible possibility of a threat to the critical asset? If found, these branches would be marked in the Threat Profile.
- For which remaining potential threats is there a negligible possibility or no possibility at all of a threat to the asset? If found, these branches would not be marked in the Threat Profile.

In addition, the team analysis also identifies additional areas of concerns, which do not exist in the generic threat profile. Readers may realize the difference between those in Figure 4-4, 4-5, 4-6 and 4-7 and those in the complete Threat Profiles.

➢ ***Check threat profiles for consistency and completeness***

OCTAVE[SM] suggests the team to examine whether the outcomes of created Threat Profile is compatible to the identified security requirement. For example, (1) if the security requirement of a critical asset is confidentiality, then in the Threat Profile, there must be a threat resulting in 'disclosure' (the related outcome); (2) if the security requirement of a critical asset is integrity, then in the Threat Profile, there must be a threat resulting in 'modification'; (3) if the security requirement of a critical asset is availability, then in the Threat Profile, there must be a threat resulting in 'loss/destruction/interruption'.

The team realized that in the Threat Profile for *Management Data* with Threat Category 'Other problems', there exists an inconsistency between security requirement 'confidentiality' of *Management Data* and the outcomes, which do not include 'disclosure'. This can be explained that the identified security for *Management Data* is driven by law and regulation of the Faculty of engineering and the university rather than by an existing threat. Thus, the team decided to skip the Threat Profile for *Management Data* with Threat Category 'Other problems'.

Finally, the team obtained the complete Threat Profiles as in Appendix C-1 to C-16 with a minor change – Management-data-based Threat Profile with 'Other Problem' is omitted. (*Note: Columns such as 'Impact', 'Probability' and 'EV/Approach' are not mentioned at this point of time).*

2.4 Phase 2 – Process 5 to 6

This phase reflects the technological view. Actually, the objective of this phase is to examine the technological weaknesses (in terms of hardware and software vulnerabilities) that can be somehow exploited via network to access data and system (e.g. UIPS, NCs, etc.). Simply put, it's not different from further checking the above-mentioned identified risks of using network to access data or system (see Figure 4-4 for reference).

Overally, as deep as the catalog of practice (see Appendix A-0) is concerned, the tasks conducted in Phase 2 completed the entire view of the center's strategic (results obtained from Phase 1) and operational security practices (some results obtained from Phase 1 plus results obtained from Phase 2). More concretely:

- System and network management
- Monitoring and auditing IT security
- Authentication and authorization
- Encryption
- Vulnerability management

It's my intention to preliminarily present this phase because:

- As discussed above, security is a management issue not a technology issue. Therefore, technology issues are just mentioned when I found it necessary to support the argument.
- Process 5 and 6 are mostly dependent on the utilization of software tools. Once those tools are available, conducting technological assessment is just a matter of time. Sources of those scanning tools, either free or commercial, are abundant. IT staff with fair knowledge of network and system can easily and conveniently carry out and interpret the assessment output. Hence, the only noteworthy point is selecting components to be evaluated.

Given these arguments, the analysis team would select the components to conduct technological assessment (Appendix A-7).

Below are some effective and popular software tools for scanning vulnerabilities:

No.	Name	Capability
1	NESSUS	Nessus is a remote vulnerability security scanner. It is plug-in-based and performs over 1200 remote security checks. It allows for reports to be generated in HTML, XML, LaTeX, and ASCII text, and suggests solutions for security problems.
2	RETINA	Commercial vulnerability assessment scanner by eEye. Retina's function is to scan all the hosts on a network and report on any vulnerability found.
3	NMAP, Port_scan, Super scan	Port scanner, pinger and hostname resolver. It can handle ping scans and port scans using specified IP ranges. It can also do finger printing of operating systems
4	Hping2, nemesis	Hping2/nemesis assembles and sends custom ICMP/UDP/TCP packets and displays any replies. It has a handy traceroute mode and supports IP fragmentation. This tool is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that block attempts using the standard utilities.

2.5 Phase 3 – Process 7 to 8

Up to this point, the team has collected data about three components of risk – threats, asset and vulnerability. After considering how critical assets are threatened and how they are technologically vulnerable, the team now broadens the view by examining how threats to the center's critical assets can affect its business objectives and mission.

Tasks to be performed are as followed:

➢ ***Identify the impact of threats to critical assets***

In this task, the analysis team is provided with a narrative description of the potential impact on the center, which reveals the influence of a threat on the center's mission and business objectives. In this case study, the following impacts are considered:

- Operation of the center
- Users' performance
- Users' confidence
- Individual property/effort
- Staff's performance
- Finance
- Rules/regulations/legal penalties
- Influence on other systems/components/devices

The results can be found in Appendix A-8 with a note that *the column 'Value'* is not mentioned at this point.

➢ ***Create risk evaluation criteria***

In this task, the team defines the center's tolerance for risk by creating evaluation criteria. These criteria are measured against which have been described in the very previous task. This, in my opinion, is quite important because the center can prioritize its known risks.

Let me spend a little space here to explain the issue of risk management. What the team analysis has done, to this point, is focusing only on the impact to measure risk. As far as I have studied, in many risk management domains, some authors have utilized the probability measure - which, as I used to somewhat discuss in Section 3.1, Chapter 2, revealed two problems. First, in information security, risk factors are extremely complex and fast changing due to the stormy evolution of IT. For example, with a massive release of software application every month, there is understandably an increasing intense of

attacks on the vulnerabilities of those software. Second, it's the lack of objective data for certain types of information security threats (e.g. human actors exploiting known vulnerabilities) that, according to Harvard Business Review (cited from Christopher and Audrey[8]), makes it difficult to develop a reliable forecast of the future. To overcome such obstacles, OCTAVE[SM] suggested a technique, namely scenario planning to define a range of threats that could affect a critical asset. Though it's unlikely to reliably predict which scenario will occur, it's fairly certain that almost everything is within the defined bounds.

I would summarize two conditions governing risk evaluation criteria:

- There is one set of evaluation criteria for all assets; the criteria are not unique to an asset.
- Evaluation criteria are created for pre-defined areas of impact, which are related to the center's key business objectives.

The risk evaluation criteria can be found in Appendix A-9.

➢ ***Evaluate the impact of threats to critical assets***

In Process 4, a Threat Profile is constructed for each critical asset. The scenarios in each Threat Profile represent those in the probable range of outcomes. Because data with respect to threat probability are limited for the scenarios, they are assumed to be equally likely (Van der Heijden; cited from Christopher and Audrey[8]). Thus, in the OCTAVE[SM] method, priorities are based on the qualitative impact values (i.e. high, medium, low) assigned to the scenarios.

The impact values assigned to the scenarios of each critical asset can be found in the Column 'Values' of Appendix A-8. The impact values will be appended into the Threat Profile later.

➢ ***Incorporating probability into the Risk***

As I have presented here and there about the difficulties when using frequency probability (or statistical data) in information security, I would raise some questions to clarify the points:

- How would an assessor estimate the probability of an attacker viewing confidential management data from the center's database? Or
- How would an assessor estimate the probability of a disgruntled student attempting to interrupt the email system or modify the center's WebPages?

To overcome such obstacles, some authors suggested to ask experts who are familiar with the system to give subjective probability. This way again encounters some problems such as the system must be in use for some period of time. Due to such difficulties, OCTAVE[SM] method (Christopher and Audrey[8]) and Charles and Shari[11] suggested to combine both frequency and subjective probability into the Risk Analysis. It means, the team analysis may ask experts to estimate the likelihood by reviewing a table based on similar system (in terms of configuration and operation). In this case study, I have got a table provided by ThaiCERT (Dr. Komain[53]), which is adapted from a relatively similar system – a computer center at the National Electronics and Computer Technology Center (NECTEC). An expert from ThaiCERT also consults the team on how to rate the system properly.

TABLE 4-6: *Ratings of Likelihood.*
Source: *Dr.Komain[53], Head – ThaiCERT, December 2003.*

Frequency	Rating	Probability Evaluation
More than once a day	10	
Once a day	9	
Once every three day	8	*High*
Once a week	7	
Once in two weeks	6	
Once a month	5	
Once every four months	4	*Medium*
Once a year	3	
Once every three years	2	*Low*
Less than once in three years	1	

After discussion, the team analysis decided to divide into three areas (high, medium, low) of probability evaluation as it can be seen in Table 4-6.

The probability evaluation will also be appended for each Threat Profile later.

➢ ***Expected Value (EV)***

The expected value (or expected loss) for a risk is the product of the potential loss that could occur (or the impact value) multiplied by its projected frequency of occurrence (or probability).

TABLE 4-7: *Expected Value Matrix*

		Probability		
		High	*Medium*	*Low*
Impact	*High*	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

According to Table 4-7, it can be easily seen that any potential catastrophic event, which has a 'low' probability and 'high' impact, would be assigned a 'medium' expected value. Likewise, a high-probability, low-impact risk would also be assigned a 'medium' expect value. Since the former is significantly different from the latter in terms of priorities, OCTAVE^{SM} suggests that the above matrix be a tool to support decision-making instead of solely depending on it.

EV of each risk is also appended in the Threat Profile.

The complete Risk Profile including asset, access (if any), actor, motive (if any), outcome, impact, probability and EV can be found from Appendix C-1 to C-16.

EV and risk management approach are important for selection of controls and control objectives in establishing ISMS.

➢ ***Risk management approach – Preparing for selection of controls***

To adequately control a threat or vulnerability, it's critical to have tools or processes in place to prevent a compromise from occurring, tools or processes in place to detect and alert the center if a compromise has occurred, and tools or processes in place to enable the center to recover from a compromise quickly and prevent future occurrences.

However, in order to have a sound and correct selection of control, it's important to understand whether controls are preventative, detective, corrective, or directive.

Definitions provided by the Computer Operations Security (URL:http://www.peacefulpackers.com/it_solutions/xisa0703.htm[53]; cited from Kevin, 2003) help to know which of the following categories a control falls into *(Note: a control may fall into more than one category)*:

Directive - The control requires an end-user or vendor to follow a policy or contract for it to be effective. What's worth mentioning here is that we cannot control whether users or vendors follow such policies or not. Hence, though policy controls are documented, they are not used in control adequacy consideration. Let's say, if the policy only applies to IT personnel (e.g. a policy to disable default user accounts on servers), it can be guaranteed that the IT personnel are following the policy. Yet, such things may not hold true for end-users or vendors.

Preventative Control - system or technology whose purpose is to prevent an attack attempt, a security incident or exploit from being successful. Also a system or technology whose purpose is to prevent a hardware failure from impacting service. Examples of preventative controls include strong passwords, firewalls, clustered servers, physical access restrictions, and encryption.

Detective Control - system or technology whose purpose is to detect an attack, a compromise, or a hardware failure and alert an administrator in an appropriate time frame. Examples of detective controls include Intrusion Detection Systems (IDS), physical security systems, centralized management tools, content monitors, virus scanners, and integrity checkers.

Corrective Control - system or technology that enables organizations to better respond to and recover from an incident, as well as prevent future occurrences. Corrective controls include incident response programs, business continuity programs and systems that record activity, events, or changes for future research.

Approach to each identified risk will be based on the effective combination of those controls. Such details are presented in *Step 5 – Selection of Controls and Controls Objectives* of Section 3 – Establishing ISMS.

3. ESTABLISHING ISMS BASED ON BS 7799 & ISO 17799

3.1 Corporate Information Security Policy

- **Definition**

It is the policy of the Engineering Computer Center (ECC) that all information assets composing of information, system, hardware, software and people shall be protected from unauthorized access, modification, fabrication, disclosure, loss or destruction, penetration, denial-of-service, subversion of security measures, or improper use as a result of espionage, vandalism, criminal, fraudulent, negligent or abusive actions. This policy should be communicated throughout the center to users (including staff, students, lecturers and visitors) in a form that is relevant, accessible and understandable.

- **Objectives & Scope**

[1] The Security Guidelines for information assets of the center are published by the risk analysis team of the ECC.

[2] These guidelines are provided as a resource to assist the center to:

(a) minimize the risk of unauthorized use, view, disclosure, fabrication or modification, loss or destruction and unavailability of the center's information assets;

(b) maximize the integrity, availability and efficacy of administering authorized access to the center's information assets; and

(c) ensure the business continuity of the center.

[3] Implementation of these guidelines should be regarded as a goal to be attained to improve the security of information assets held by the ECC. Since no system can be absolutely secure, application of the guidelines does not fully guarantee the confidentiality, integrity or availability of ECC's information assets.

[4] The ECC must make decisions concerning security issues based on an objective assessment of potential risks. Such risks must be balanced against the costs and other organizational priorities. Responsibility and accountability for the security of the center's information assets rests solely with the center.

[5] This policy applies to all operating units of the center with direct, indirect, or implied access to information assets owned by or entrusted to the center.

- **Principles of information security**

These guidelines have been produced in consideration of the following fundamental principles:

[1] Staff and users (i.e. lecturers, students) have a right to privacy of information assets of the center. Such information assets cannot be disclosed without their authorization;

[2] ECC's staff require access to information assets for the delivery of services to the users;

[3] Users (i.e. lecturers, students) require the availability and integrity of information assets for their work;

[4] The ECC (e.g. operating units) requires the entire information assets to manage resources and programs for the delivery of effective services;

[5] Faculty of Engineering and University may require the ECC's information assets to develop, promote and manage the center's resources at a macro level.

[6] Some units or entities existing within the Faculty environment may require ECC's information assets to support their operation and development.

- **Regulatory requirements**

All staff and users are responsible for becoming familiar and compliant with this policy and related standards, guidelines, and procedures. Additionally, staff are responsible for reporting any known or observed deficiencies in this policy's control mechanisms. Such deficiencies must be documented and reported to the cognizant manager of the center for improvement.

Information assets are ECC's vital resources that require protection commensurate with their value. Mechanisms shall be in place to protect these assets from accidental or deliberate modification, destruction, unauthorized disclosure, interruption or other malfeasance to ensure confidentiality, integrity, and availability.

- **Explanation**

This policy addresses some issues to be taken into account:

[1] Security education requirements: This is to equip staff (and even users) with up-to-date knowledge of information security. Once they recognize and grasp such issues, they'll be more active and efficient to respond to risk and maintain business continuity.

[2] Business continuity management: This means the center manages to provide computing facilities for users continually. Since this is the primary concern of the

center, the center's resources are fully devoted to ensure the operational availability efficiently.

[3] Consequences of security policy violations: These range from minor impact such as loosing individual's property, effort and performance to huge impact such as suspending the center's operation, financial loss, regulatory violations or undermining users' confidence.

- **Risk management context**

These guidelines address the following risks to ECC's information assets and provide practical suggestions to assess and minimize such risks:

[1] Unauthorized disclosure

[2] Unauthorized or accidental modification (or fabrication)

[3] Unauthorized removal

[4] Unauthorized or accidental destruction

[5] Interruption in access to critical information assets

- **Responsibilities**

These guidelines are intended for any individual or operating unit (within the center) who is responsible for the management of information assets. In general, the guidelines are directed to anyone whose responsibilities include the following:

[1] Utilization of ECC's information assets

[2] Control of access to ECC's information assets by the center's staff and users including lecturers and students

[3] Protection of information assets from unauthorized access, modification or destruction

[4] Analysis and distribution of ECC's information assets such as management data, as appropriate, to other entities within the Faculty of Engineering or the University.

Responsibility of Administration Unit Manager

- The identification and protection of information assets within their sphere of influence
- Insure staff awareness of this policy and supporting procedures, guidelines, and standards
- Review and reinforce compliance with established security controls

Responsibility of Technical Team Manager

- Oversee the protection of information assets of the center
- Develop and implement security policies and standards
- Serve as consultant and assist management in all matters relating to information security for the protection of information assets
- Ensure that system, network, and application security requirements are in compliance with this policy

- **Supporting documentation**
  - ISO 17799: 2000
  - Other internationally recognized printed and online documents (See References).

3.2 Scope of the ISMS

- **Process**

The process to establish the scope and context of ISMS is based on PDCA (Plan-Do-Check-Act) model, where:

- *Plan:* understanding business information security requirements and the need to establish policy and objectives for information security;
- *Do:* implementing and operating controls in the context of managing the center's overall business risk;
- *Check:* monitoring and reviewing the performance and effectiveness of the ISMS;
- *Act:* continual improvement based on objective measurement;

- **Organizational context**

The ISMS is developed within the context:

- The Engineering Computer Center is the only computing facilities serving the needs of study and communication of lecturers and students at the Faculty of Engineering.
- The ECC's personnel include 13 staffs, dividing into administration unit and technical team.
- Administration unit is in charge of managing the center in terms of operating and protecting the entire facilities.
- Technical team is responsible for keeping the computing infrastructure running continually.

- **Approach to information security risk management**

The approach is based on the OCTAVE[SM] – a self-driven and asset-based risk evaluation method.

- **Criteria for information security risk evaluation**

Criteria for evaluating risk can be found in Appendix A-9.

- **Identification of information assets**

These guidelines apply to the utilizing and maintaining of the ECC's information assets regardless of the technology platform or mode used. These include:

- *Management data:* All data that are crucial for the daily operational activities of the center. For example: users' and groups' information (i.e. identification, password, privileges and services), staff's information (i.e. identification, password, privileges and task information), information of center's activities with internal and external organizations and financial and accounting records.
- *Users' data:* Personal and academic data of students and lecturers.
- *User Information Processing System (UIPS):* This system helps to manage user-related data (i.e. accounts, storage, printing, FTP services, etc.) including email system at ECC.
- *Personal computers (PCs):* All PCs that are currently used at the center.
- *Network and Networking Components (NCs):* Attention is paid to all networking components such as servers, routers, bridges, switches, hubs and cables.
- *Technical team:* Technical team possess expertise and skills critical that are for the daily operation of ECC in terms of managing, maintaining and developing the computing facilities.

3.3 Risk Analysis

Once the scope is defined, the center must undertake a risk assessment to evaluate the risk and threats to its information assets and their respective impacts to the center. When evaluating risks, the center would take into account at a minimum both the severity of the risks and their likelihood of occurrence.

- **Identification of assets, threats, impacts and probability**

Details on conducting risk assessment can be found from Section 2.1 to Section 2.5 (excluding Expected Value – EV).

- **Risk assessment results**

The obtained results can be found in Appendix C excluding EV (Expected Value), which will be discussed in Step 4 – Risk Management.

- **Conclusion**
  - The selected information assets are most critical to the operation of the center. Although minimizing or even eliminating all the risks is impossible, *focusing on critical a few* in information security implies that the majority of the risk that the center is exposed to can be substantially reduced by implementing the few most important procedures. By focusing the security time and resources on these areas, maximum impact is achieved in a short amount of time. This fact reflects the 80/20 rule known as Pareto principle.
  - Threat sources used in this risk assessment are identified by security experts. However, due to the fast changing of IT, it's important to review and update the threat source to enhance the reliability of the risk assessment.
  - In addition to identifying threats, this method also captured knowledge of current organizational security practices and organizational vulnerabilities. There are two advantages to be highlighted. First, many other methods overlook this issue since they just focus on technological vulnerabilities rather than paying more attention to organizational vulnerabilities – the core of information security. Second, this kind of information is of utmost significance to select controls and controls objectives in Step 5.
  - Impact level description is flexible and based on the characteristics of business, assets and technology of the center. Once those factors are modified, impact level description is also re-defined.
  - To enhance reliability, incorporating possibility into risk assessment requires two points. First, the familiar system must be as close to the currently-evaluated system as possible. Second, subjective probability must be more accurate. This is feasible with experienced security experts.

3.4 Risk Management

Next, the center determines how to manage the risks. Based on its information security policy and the degree of assurance required, the center prioritizes the risks in terms of Expected Value (EV) or Expected Loss.

- **Approach to risk management**

The risk management approach is:

- *Reduction:* by controlling risk with available resources (i.e. staff, time, money, etc.) and preparing to deal with the loss if it occurs; or
- *Acceptance:* by doing nothing.

- **Degree of assurance**

The impact levels as well as the probability – the two key components to prioritize the risk – are highly reliable. High reliability is achieved because of thorough and correct collection of data during risk assessment.

- **Risk prioritization**

Risk prioritization is determined in terms of the Expected Value (EV). There are three levels of EV: high, medium and low. Results can be found in Appendix C.

- **Areas of risk to be managed**
  - For users' data and UIPS: integrity
  - For management data: confidentiality
  - For PCs, NCs, technical team: availability

3.5 Selection of Controls

The complete risk treatment framework showing for each identified risk is:

- The method selected for treating the risk;
- Select controls and objectives from BS 7799-2: 2002 and ISO 17799:2000;
- Additional controls from other internationally recognized sources;
- Rationale for selection;
- Time frame over which the proposed controls are to be implemented;

➢ ***Risk 1 – Human actors use network to access users' data – TABLE 4-8***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 1. Password use *(Appendix B-1)*	To guide users about using password securely and properly (Directive and Preventive)	1 week	1 Directive 3 Preventive 1 Detective
Clause 2. User password management *(Appendix B-1)*	To prevent unauthorized access to users' data (Preventive)	1 month	1 Corrective *Adequacy: Strong*
Clause 3. Review of user access rights *(Appendix B-1)*	To enhance the effectiveness of password management system (Preventive, Detective)	2 months	
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	

➢ ***Risk 2 – System problems to threaten users' data – TABLE 4-9***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 5. Access control to program source library *(Appendix B-2)*	To reduce the potential for corruption of computer programs (Preventive, Corrective)	2 weeks	6 Preventive 3 Detective 3 Corrective *Adequacy: Strong*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	
Clause 7. Controls against malicious software *(Appendix B-2)*	To protect the integrity of software and information (Detective, Preventive).	1 months	

Clause 8. Reporting security incidents *(Appendix B-2)*	To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents (Detective).	1 months	
Clause 9. Reporting software malfunctions *(Appendix B-2)*	To minimize the damage from software malfunctions by detecting errors (Detective)	2 weeks	
Clause 15. Review and audit of computing system *(Appendix B-5)*	To prevent hardware failures (Preventive)	4 months	
Clause 10. Cryptographic controls *(Appendix B-2)*	To protect the confidentiality and integrity of information (Preventive)	2 months	
Clause 11. Support for purchased information assets *(Appendix B-2)*	To avoid hardware and software defects (Preventive)	4 months	

➢ ***Risk 3 – Other problems to threaten users' data – TABLE 4-10***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 12. Power supplies *(Appendix B-3)*	To ensure operational continuity of information assets (e.g continuous accessing to management data and users' data, operational continuity of systems, etc.) (Preventive)	1 month	2 Preventive 2 Corrective *Adequacy: Need testing.*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 29. Policy on the technical team's commitment and common objectives *(Appendix B-11)*	To enable management to establish commitment and common objectives, which guide them how to prevent incidents from occurring; effectively respond to incidents; and quickly recover from incidents (Preventive, Corrective).	2 weeks	

➢ ***Risk 4 – Human actors use network to access management data – TABLE 4-11***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 13. Policy for accessing to business information & application system *(Appendix B-4)*	Avoid unauthorized disclosure, modification or destruction (Preventive, Corrective).	1 month	3 Preventive 1 Detective 3 Corrective *Adequacy: Strong*
Clause 14. Quality of processing management data *(Appendix B-4)*	This policy is to ensure the integrity of the management data, which is important to the operational stability of the center (Preventive, Detective, and Corrective).	2 weeks	
Clause 10. Cryptographic controls *(Appendix B-2)*	To protect the confidentiality and integrity of information (Preventive)	2 months	
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	

➢ ***Risk 5 – System problems to threaten management data – TABLE 4-12***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 5. Access control to program source library *(Appendix B-2)*	To reduce the potential for corruption of computer programs (Preventive, Corrective)	2 weeks	6 Preventive 3 Detective 3 Corrective *Adequacy: Strong*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	
Clause 7. Controls against malicious software *(Appendix B-2)*	To protect the integrity of software and information (Detective, Preventive).	1 months	
Clause 8. Reporting security incidents *(Appendix B-2)*	To minimize damage from security incidents & malfunctions, and to monitor and learn from such incidents (Detective).	1 months	
Clause 9. Reporting software malfunctions *(Appendix B-2)*	To minimize the damage from software malfunctions by detecting errors (Detective)	2 weeks	
Clause 15. Review & audit of computing system *(Appendix B-5)*	To prevent hardware failures (Preventive)	4 months	
Clause 10. Cryptographic controls *(Appendix B-2)* Clause 16. Policy on the use of cryptographic controls *(Appendix B-5)*	To protect the confidentiality and integrity of information (Preventive).	2 months	
Clause 11. Support for purchased information assets *(Appendix B-2)*	To avoid hardware and software defects (Preventive)	4 months	

➢ ***Risk 6 – Human actors use network to access UIPS – TABLE 4-13***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 13. Policy for accessing to business information & application system *(Appendix B-4)*	Avoid unauthorized disclosure, modification or destruction (Preventive, Corrective).	1 month	4 Preventive 2 Detective 3 Corrective *Adequacy: Strong*
Clause 14. Quality of processing management data *(Appendix B-4)*	This policy is to ensure the integrity of the management data, which is important to the operational stability of the center (Preventive, Detective, and Corrective).	2 weeks	
Clause 10. Cryptographic controls *(Appendix B-2)* Clause 16. Policy on the use of cryptographic controls *(Appendix B-5)*	To protect the confidentiality and integrity of information (Preventive)	2 months	
Clause 17. Information access restriction *(Appendix B-6)*	To prevent unauthorized access to information held in information system (Preventive).	1 month	
Clause 18. Monitoring system access & use *(Appendix B-6)*	To detect unauthorized activities (Detective)	2 weeks	
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	

➢ ***Risk 7 – System problems to threaten UIPS – TABLE 4-14***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 5. Access control to program source library *(Appendix B-2)*	To reduce the potential for corruption of computer programs (Preventive, Corrective)	2 weeks	1 Directive 5 Preventive 3 Detective 3 Corrective
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	*Adequacy: Strong*
Clause 7. Controls against malicious software *(Appendix B-2)*	To protect the integrity of software and information (Detective, Preventive).	1 months	
Clause 8. Reporting security incidents *(Appendix B-2)*	To minimize damage from security incidents & malfunctions, and to monitor and learn from such incidents (Detective).	1 months	
Clause 9. Reporting software malfunctions *(Appendix B-2)*	To minimize the damage from software malfunctions by detecting errors (Detective)	2 weeks	
Clause 15. Review & audit of computing system *(Appendix B-5)*	To prevent hardware failures (Preventive)	4 months	
Clause 10. Cryptographic controls *(Appendix B-2)* Clause 16. Policy on the use of cryptographic controls *(Appendix B-5)*	To protect the confidentiality and integrity of information (Preventive).	2 months	
Clause 11. Support for purchased information assets *(Appendix B-2)*	To avoid hardware and software defects (Preventive)	4 months	
Clause 19. Policy on the use of email *(Appendix B-7)*	To prevent risks created by using e-mails (Directive, Preventive)	1 week	

➢ ***Risk 8 – Other problems to threaten UIPS – TABLE 4-15***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 12. Power supplies *(Appendix B-3)*	To ensure operational continuity of information assets (e.g continuous accessing to management data and users' data, operational continuity of systems, etc.) (Preventive)	1 month	2 Preventive 2 Corrective *Adequacy: Need testing.*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 29. Policy on the technical team's commitment and common objectives *(Appendix B-11)*	To enable management to establish commitment and common objectives, which guide them how to prevent incidents from occurring; effectively respond to incidents; and quickly recover from incidents (Preventive, Corrective).	2 weeks	

➢ ***Risk 9 – Human actors use network to access NCs – TABLE 4-16***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 13. Policy for accessing to business information & application system *(Appendix B-4)*	Avoid unauthorized disclosure, modification or destruction (Preventive, Corrective).	1 month	2 Preventive 1 Detective 3 Corrective *Adequacy: Strong*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 20. Segregation of duties *(Appendix B-8)*	To reduce the risk of accidental or deliberate system misuse (Detective).	2 weeks	
Clause 21. Network controls *(Appendix B-8)*	To ensure the safeguarding of information in networks and the protection of the supporting infrastructure (Preventive, Corrective).	2 months	

➢ ***Risk 10 – Human actors physically access to NCs – TABLE 4-17***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	2 Preventive 1 Detective 3 Corrective *Adequacy: Strong*
Clause 22. Physical security controls *(22.1, 22.2, 22.4, 22.5 – Appendix B-9)*	To prevent unauthorized access, damage and interference to physical assets of the center (Preventive).	2 months	
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 23. Reporting security weaknesses *(Appendix B-9)*	To prevent and detect modification, destruction or interruption (Corrective, Detective).	2 weeks	

➢ ***Risk 11 – System problems to threaten NCs – TABLE 4-18***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 5. Access control to program source library *(Appendix B-2)*	To reduce the potential for corruption of computer programs (Preventive, Corrective)	2 weeks	6 Preventive 4 Detective 5 Corrective *Adequacy: Strong*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 7. Controls against malicious software *(Appendix B-2)*	To protect the integrity of software and information (Detective, Preventive).	1 months	
Clause 8. Reporting security incidents *(Appendix B-2)*	To minimize damage from security incidents & malfunctions, and to monitor and learn from such incidents (Detective).	1 months	
Clause 9. Reporting software malfunctions *(Appendix B-2)*	To minimize the damage from software malfunctions by detecting errors (Detective)	2 weeks	
Clause 11. Support for purchased information assets *(Appendix B-2)*	To avoid hardware and software defects (Preventive)	4 months	
Clause 27. Physical information asset maintenance (Appendix B-10)	To ensure availability and integrity of physical information assets (Preventive).	1 month	
Clause 23. Reporting security weaknesses *(Appendix B-9)*	To prevent and detect modification, destruction or interruption (Corrective, Detective).	2 weeks	
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	

Clause 24. Documented operating procedures *(Appendix B-10)* Clause 25. Operational change control *(Appendix B-10)*	To reduce the likelihood of encountering operating/network administration software defects and hardware defects (Preventive).	2 weeks	
Clause 26. Incident response management procedures *(Appendix B-10)*	To better response to incident such as modification, loss/destruction or interruption (Corrective)	1 month	

➢ ***Risk 12 – Other problems to threaten NCs – TABLE 4-19***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 12. Power supplies *(Appendix B-3)*	To ensure operational continuity of information assets (e.g continuous accessing to management data and users' data, operational continuity of systems, etc.) (Preventive)	1 month	3 Preventive 3 Corrective *Adequacy: Need testing.*
Clause 4. Backup data *(Appendix B-1)*	To quickly and fully recover the information lost/destroyed due to security incidents (Corrective).	1.5 months	
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	
Clause 22. Fire protection *(22.3 – Appendix B-10)*	To protect physical information assets from damage and respond to natural disaster (Preventive, Corrective)	2 weeks	
Clause 22. Evacuation procedures *(22.7 – Appendix B-10)*		2 weeks	
Clause 29. Policy on the technical team's commitment and common objectives *(Appendix B-11)*	To enable management to establish commitment and common objectives, which guide them how to prevent incidents from occurring; effectively respond to incidents; and quickly recover from incidents (Preventive, Corrective).	2 weeks	

➢ ***Risk 13 – Human actors physically access to PCs – TABLE 4-20***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	3 Preventive 1 Detective 2 Corrective *Adequacy: Strong*
Clause 27. Physical information asset maintenance *(Appendix B-10)*	To ensure availability and integrity of physical information assets (Preventive).	1 month	
Clause 22. Physical security controls *(22.1, 22.2, 22.4, 22.5 – Appendix B-9)*	To prevent unauthorized access, damage and interference to physical assets of the center (Preventive).	2 months	
Clause 23. Reporting security weaknesses *(Appendix B-9)*	To prevent and detect modification, destruction or interruption (Corrective, Detective).	2 weeks	

➢ ***Risk 14 – System problems to threaten PCs – TABLE 4-21***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 7. Controls against malicious software *(Appendix B-2)*	To protect the integrity of software and information (Detective, Preventive).	1 months	6 Preventive 3 Detective 3 Corrective
Clause 8. Reporting security incidents *(Appendix B-2)*	To minimize damage from security incidents & malfunctions, and to monitor and learn from such incidents (Detective).	1 months	*Adequacy: Strong*
Clause 15. Review & audit of computing system *(Appendix B-5)*	To prevent hardware failures (Preventive)	4 months	
Clause 11. Support for purchased information assets *(Appendix B-2)*	To avoid hardware and software defects (Preventive)	4 months	
Clause 27. Physical information asset maintenance (Appendix B-10)	To ensure availability and integrity of physical information assets (Preventive).		
Clause 23. Reporting security weaknesses *(Appendix B-9)*	To prevent and detect modification, destruction or interruption (Corrective, Detective).	2 weeks	
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's assets (Preventive, Corrective).	4 months	
Clause 25. Operational change control *(Appendix B-10)*	To reduce the likelihood of encountering operating/network administration software and hardware defects (Preventive).	2 weeks	
Incident management response *(Appendix B-10)*	To better response to incident such as modification, loss/destruction or interruption (Corrective)	1 month	

➢ ***Risk 15 – Other problems to threaten PCs – TABLE 4-22***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 12. Power supplies *(Appendix B-3)*	To ensure operational continuity of information assets (e.g continuous accessing to management data and users' data, operational continuity of systems, etc.) (Preventive)	1 month	4 Preventive 3 Corrective *Adequacy: Need testing.*
Clause 6. Inventory of physical assets *(Appendix B-2)*	To maintain appropriate protection of the center's information assets (Preventive, Corrective).	4 months	
Clause 22. Fire protection *(22.3 – Appendix B-10)*	To protect physical information assets from damage and respond to natural disaster (Preventive, Corrective)	2 weeks	
Clause 22. Evacuation procedures *(22.7 – Appendix B-10)*		2 weeks	
Clause 29. Policy on the technical team's commitment and common objectives *(Appendix B-11)*	To enable management to establish commitment and common objectives, which guide them how to prevent incidents from occurring; effectively respond to incidents; and quickly recover from incidents (Preventive, Corrective).	2 weeks	

➢ ***Risk 16 – Other problems to technical team - TABLE 4-23***

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply	Control Adequacy
Clause 28. Information security management training for staff *(Appendix B-11)*	To enable management to provide training on up-to-date best practices of security and on how to respond effectively and recover quickly from incidents (Preventive, Corrective).	2 month	2 Preventive 2 Corrective *Adequacy: Need testing.*
Clause 29. Policy on the technical team's commitment and common objectives *(Appendix B-11)*	To enable management to establish commitment and common objectives, which guide them how to prevent incidents from occurring; effectively respond to incidents; and quickly recover from incidents (Preventive, Corrective).	2 weeks	

To be more effective, the ISMS should be enhanced with additional controls as followed (*TABLE 4-24*):

Select controls & control objectives	Rationale for selection	Time frame to prepare & apply
Clause 30. Management information security forum *(Appendix B-12)*	To enhance the effectiveness of information security management within the center (Preventive, Corrective).	1 month
Clause 31. Personnel security *(Appendix B-12)*	to reduce the risks of human error, theft, fraud or misuse of information assets (Preventive)	1.5 months
Clause 32. Disciplinary process *(Appendix B-12)*	To prevent staff from compromising the center's information assets (Preventive)	2 weeks
Clause 33. Contingency planning *(Appendix B-12)*	To strengthen the effectiveness of responding to security breaches and incidents leaving serious impact on the center's operation. (Corrective)	1.5 months

Clause 34. Business continuity program *(Appendix B-12)*	To counteract interruptions to operational activities and to protect critical operational processes from the effects of major failures or disasters. (Corrective)	2 months

3.6 Statement of Applicability

The reasons for the selection of controls are clearly defined in column 2 (from left) in the previous step.

There are two exceptions for the applicability:

- For the risk profile of NCs concerning the threat actor of Internet connection shutdown (CUNET Web server malfunctioned), there is no control to minimize this risk, which is assessed as 'High Expected Valuation' in the risk assessment (see Appendix C-11). Such system problem is not under control of the center.
- For the risk profile of technical team concerning the threat actor of insufficient budget to ensure the team's effectiveness, there's no selection of controls to minimize this risk, which is assessed as 'High Expected Valuation' in the risk assessment (see Appendix C-16). Such financial problem is currently over the capability of the center.

To this point, the ISMS has been completely established. To make sure that the system is working properly and effectively, it's crucial to go to the next phase – Check phase. However, before monitoring and reviewing the ISMS, the center must implement and operate the newly-established ISMS.

4. THE DO-CHECK-ACT PHASES

Once the ISMS has been designed and implemented, it is important that the system is regularly reviewed and monitored to test that it not only remains effective but to identify and fix any problems and weaknesses as part of the continual improvement process. Senior management would be expected to be part of these phases. Brief introduction of the phases is:

- **The Do-Phase (implementing and operating the ISMS)**
  In this phase, the center's objective is to keep the ISMS 'running' by identifying appropriate action plan, implementing the selected controls and training and awareness program. Additionally, managing resources (i.e. time, budget, personnel, etc.) is taken into account. All actions facilitate the prompt detection of and response to security incidents.

- **The Check-Phase (monitoring and reviewing the ISMS)**
  In this phase, the center's objective is to detect errors, failed and successful security breaches and incidents promptly and determine how to resolve those problems. Moreover, the center would regularly conduct ISMS audits to enhance the effectiveness of the system.

- **The Act-Phase (maintaining and improving the ISMS)**
  After identifying problems of the existing ISMS, the center would enhance the ISMS's effectiveness by taking appropriate corrective and preventive actions.

This *Act-Phase* finishes the continuous PDCA cycle and re-starts a new PDCA cycle with the *Plan-Phase*. Throughout the cycle, all procedures and steps are digitally documented.

5. CONCLUSION

By properly and correctly conducting risk assessment, the center has achieved the two objectives:

- Identifying the threat actors, the associated impacts and the probabilities of security risks occurring to the center's information assets, and
- Using the assessment results (e.g. in terms of risk prioritization), to establish an ISMS that efficiently controls the identified risks.

Such a large amount of work is quite significant and worthy since it proves that the center has stridden a long way in solving the security issues. They look into themselves to find out weaknesses and go further by seeking out a complete solution for improving these problems. As it can be seen from this presentation, conducting a successful risk assessment is, in effect, not a Mickey-mouse work. Even tougher is how to work them out by creating and bring the system into existence. Indeed, as Peter Coffee[34] – a technology editor of EWEEK – concluded "It's not the job of IT administrators to deploy every available security tools; it's their job to assess the balance between degree of protection on the one hand and likelihood of consistent and correct use of systems on the other".

Only when we have a thorough grasp of this idea will we be quite successful with our self-established model.