CHAPTER 5

CONCLUSION

Rather than responding to each year's security trend, companies should start from a carefully considered written security policy stating exactly what they need to achieve in order to protect their specific assets".
Wayman Thurman[35], Director
North American Sales at Blue Lance.

1. ANSWERS TO RESEARCH QUESTIONS

Answering to the questions in Section 3, Chapter 1 helps to summarize the content of this study:

1. *What is an ISMS and why to develop it?*

An ISMS is a mechanism in which people, processes and computing infrastructure interact each other, aiming at securing organization's most critical information assets in terms of availability, integrity and confidentiality.

There are a few reasons for establishing an ISMS:

- The model of Quality Management System (QMS), for over a decade, has proven its effectiveness of enhancing the quality of service and product provided by worldwide enterprises. Yet, in this knowledge economy, the growth or survival of the organization is not only limited to ensuring the quality but also extended to protecting information. Indeed, if we wish to rank the assets, next to personnel – the most valuable one – is unarguably the information. which is considered the lifeblood of each organization. Day in day out, numerous information security breaches and incidents as well as their associated consequences overwhelm mass media, heavily striking the enterprises' operation. Given that context, establishing an ISMS is a must since it enables to maintain the organization's information security posture, thereby minimizing financial loss, keeping the stability of internal and external business activities and most significantly, the customers' credit.
- The mutual confidence between partners is remarkably increased. This, in my opinion, is particularly important when organizations wish to interconnect electronically in the global market.

- Compliance with legal and contractual specifications. This matter is ultimately significant when considering the context of doing business in developed countries.
- Faster and easier recovery from attacks and improved ability to survive disaster.

2. Which approach will be used to conduct risk assessment? Why?

Risk assessment method, namely the OCTAVE^{SM} is selected in this study. As compared with numerous methods currently available, the OCTAVE^{SM} seems to be dominant mainly because:

- its methodology is quite different from many known methods in terms of structure. OCATVE^{SM} starts with senior management's view and ends with technical view. This, in effect, reflects the point of view *"Security is a management issue not a technological one"*,
- it's flexible (in terms of creating a basic set of criteria) and thus, can be uniquely tailored to each specific context of the organization,
- it incorporates organizational issues related to how people use the computing facilities to meet the business objectives of the organization,
- OCTAVE^{SM} is an asset-driven evaluation approach, framing the organization's risks in the context of its assets. 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,
- it is a qualitative approach - a properly and conveniently-implemented way for IT context.
- it focuses on practice-based mitigation using recognized, good security practices. For instance, the BS 7799:1995 is among important sources to create this catalog.

Obviously, the benefits achieved by adopting this method is quite convincing. More importantly, it enables organization to correctly assess their security posture.

3. What are the ECC's information security threats and vulnerabilities?

Overally, threats that occur to ECC's information assets derive from many sources:

- *Deliberate human actors:* people, either inside or outside the organization, may deliberately affect the information assets;
- *Accidental human actors:* people, either inside or outside the organization, may deliberately affect the information assets;

- *System problems:* hardware defects, software defects, unavailability of related system, malicious codes or programs (i.e. viruses, Trojan horses, worms, back-door, spyware, Spam and junk mail, etc.);
- *Other problems:* power outage, ISP or telecommunication unavailable, natural disaster;

4. How and where do those threats come from?

➢ *For human actors,* they can use *either network or physical access* to influence on information assets.

  - *Using network access:* intruder or attacker exploit technological vulnerabilities in terms of system and software flaws to access sensitive or confidential data or system to perform unauthorized tasks.
  - *Using physical access:* intruder or attacker exploit physical security weaknesses in the organization to access data, hardware or system to perform unauthorized tasks.

➢ *The system problems* concern any problems related to IT, which have negative influences on the operation of information assets.

➢ *Other problems* concern any problems not mentioning system or human actors.

5. What are the consequences of those threats?

There are four consequences ranging from minor impact to huge impact:

➢ *Disclosure:* Unauthorized people can read, view, print data or even simply know that a particular information asset exists within the center. This consequence can be considered as a breach of *'confidentiality'* or *'secrecy'* or *'privacy'*.

➢ *Modification/Fabrication:* Information assets of the center are modified by either unauthorized people or authorized people in unauthorized manner. This consequence can be understood as an action or behavior of writing or creating (i.e. data), fabricating (i.e. Email system), changing status (i.e. PCs, Networking, etc.).

➢ *Loss/destruction:* Information assets of the center are destroyed or lost. For example, a hardware or system is removed or destroyed; important management data are lost.

- *Interruption/Unavailability/Denial of service:* Accessing to information assets of the center (i.e. Network, PCs or application system) is interrupted or unavailable for a period of time. This can be interpreted as a *'Denial of service'*.

6. What are the impacts? What are ECC's threat profiles?

The impacts on the center, following the above mentioned consequences, are:

- *ECC's operation* – The center's operation level is decreased or suspended.
- *User's performance* – User's performance on information assets (i.e. PCs) is negatively affected.
- *User's confidence* – User's confidence is negatively influenced or undermined.
- *Staff's performance* – Staff' performance on information assets (i.e. PCs) is negatively affected.
- *Rules/Regulations/Legal penalties* – Security incidents violate the rules or regulations required by Faculty of Engineering or the University.
- *Financial* – The center suffers a financial loss, which may not be redeemable.
- *Individual property/effort* – User's or staff' effort or property is lost/destroyed.
- *Influences on other systems/Components/Devices* – Other system/Components/Devices experienced negative influences or suspended due to security incidents.

Threat Profiles provide the center with an in-depth view into the risk occurring to the center's information assets. Threat Profile is tailored from a Generic Threat Profile for each of identified information asset and include the following information;

- *Assets:* critical information assets of the center. In this study, there six critical information assets such as users' data, management data, UIPS, PCs, NCs and the technical team;
- *Access:* either physical or network ;
- *Actor:* people or things that cause incidents or breaches;
- *Motive:* either deliberately or accidentally;
- *Outcome:* the four consequences mentioned above;
- *Impact:* the eight impact areas described above;
- *Probability:* the likelihood of occurrence of an incident or breach;
- *Expected Loss or Expected Value (EV) and Approach to Risk:*

Based on the information represented on those Threat Profiles, management would make decision on how to control the identified risks.

7. Which model of ISMS will be adopted? Why choose them?

The ISMS model is adopted from the BS 7799-2: 2002 and its companion ISO/IEC 17799: 2000.

ISO/IEC 17799:2000 (Guidance Standard) is the standard code of practice for information security management and can be regarded as a comprehensive catalogue of good security practices to follow. ISO/IEC 17799 is an internationally recognized Information Security Management Standard. It was first published by the International Organization for Standardization (ISO) in December 2000. Whilst there are many other "Guidelines" and "Best Practices", ISO 17999 is the only standard for *Information Security Management*.

BS 7799-2: 2002 (certification standard), released in December 2002, is the specification document against which an organization is measured for compliance and subsequent certification. BS7799 tells organizations how to apply ISO/IEC 17799 and most importantly, how to develop, implement and operate, monitor and review, maintain and improve an ISMS.

The rationale for choosing these standards to establish ISMS are:

- Differing from many available models that presented more technical point of view, the BS 7799 suggested an approach to develop an ISMS that is of organizational point of view.
- These criteria are used as a basis for implementing different software systems.
- ISO 17799 is quite flexible. It proposes setting up different safeguards, but the real attention is put to organizational changes.
- According to various academics as well as practitioners, these two criteria, presently recognized by more and more organizations throughout the world, will soon be integrated into the existing management systems such as QMS or EMS, which have been proving the huge successes in the industry.

8. How to develop an efficient ISMS? What are the components of an ISMS based on ISO 17799:2000 and BS 7799-2:2002?

The BS 7799 based on the BS 7799-2 is based on "Plan-Do-Check-Act" approach as followed:

- ***Plan (develop the ISMS):*** Establish a security policy, along with objectives, goals, processes and procedures for managing risk and improving information security, in order to deliver results in keeping with the center's overall objectives and policies.
- ***Do (implement & operate the ISMS):*** Implement and operate the security policy, controls, processes and procedures.
- ***Check (monitor & review the ISMS):*** Assess, and where applicable measure, process performance against security policies, objectives and practical experience. Report the results to management for review.
- ***Act (maintain and improve the ISMS):*** In order to continually improve the ISMS, carry out corrective and preventative action based on the results of the management review.

BS 7799-2: 2002 instructs organizations how to develop an efficient ISMS using control objectives described in ISO 17799: 2000. Developing an ISMS requires a six-step process as followed:

1. *Corporate Information Security Policy:* This step is to provide management direction and support for information security.
2. *Scope of the ISMS:* This step is to define the boundaries of ISMS in terms of the characteristics of the business, the center, its assets and technology.
3. *Risk Analysis:* This step is to identify the threats and vulnerabilities of the center and information processing facilities and assess the likelihood of their occurrence and the impact to the business goals.
4. *Risk Management:* After identifying risk, the center assesses the business harm resulting from security failure and the likelihood of occurrence. Besides, the center estimates the levels of risks and determines whether the risk is acceptable or requires treatment using the criteria established.
5. *Selection of Controls:* Appropriate control objectives from ISO/IEC 17799 and other internationally recognised documents are selected and justified on the basis of the conclusion of the risk assessment.
6. *Statement of Applicability:* This step states the reasons for the selection of the controls for the ISMS.

- ***Risk 1 – Human actors use network to access users' data***

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 1 Corrective *<u>Adequacy:</u> Strong*
Clause 2. User password management *(Appendix B-1)*	To prevent unauthorized access to users' data (Preventive)	1 month	
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***

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 *<u>Adequacy:</u> 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***

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***

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***

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 *<u>Adequacy:</u> 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*

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***

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 *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 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***

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***

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 <u>Adequacy:</u> *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***

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 *<u>Adequacy:</u> 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***

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***

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 Adequacv: *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***

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***

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 *<u>Adequacy:</u> Strong*
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 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***

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*

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:

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

9. What needs to be taken into consideration before and after the implementation of this ISMS at the center?

Before the implementation of ISMS, there should be:

- visible support and commitment from management;
- effective dissemination of information security issues to all staff;
- a good and feasible schedule for establishing the ISMS regarding all issues such as budget, time-scale, personnel, other resources, etc.
- distribution of guidance on information security policy and standards to all concerned staff and management;
- a good preparation for a comprehensive and balanced benchmark system (e.g. it could be like the balanced scorecard) which is used to evaluate performance in information security management and feedback suggestions for improvement;
- high unanimity on the detailed action plan achieved by staff from both business unit and technical team;
- contingency plan in case that the implementation cannot be carried out or is suspended;

After the implementation of ISMS, it's crucial for management to conduct review of the ISMS implementation routinely. This can be done by the effective use of the benchmark system. Weaknesses or inappropriateness will be identified to improve the ISMS's effectiveness.

2. LESSONS LEARNED FROM THIS STUDY

This study has enabled me to elicit some thoughts that are worthy to discuss:

2.1 Information Security Risk Assessment

- ***A "Top-down" risk assessment approach***

The data-collecting processes conducted from Process 1 to 6 in the OCTAVE^{SM} follows a 'top-down' approach. First, the process begins with senior management from a managerial look (i.e. Process 1 to 3) and ends with examining computing infrastructure from a technical look (i.e. Process 5 and 6). Although the approach goes against the conventional and popular approach that runs from the root of information security by scanning vulnerabilities up to management, it reveals the essence of information security - a management issue.

- ***Focus on critical a few***

As it can be seen from the previous presentation of focusing on critical a few – a prominent characteristics of OCTAVE^{SM} method, I would highlight some issues regarding this aspect in information security.

First, it must be confirmed that eliminating or minimizing all the risks, especially the area of information technology, is impossible. Some risks might put the center out of business, whereas the other might merely be a nuisance. Given this fact, correct selecting the objectives to be protected is the key since it ensures to effectively control as many risk, which, in effect, threaten the survival or growth of the center, as possible. The 80/20 rule, better known as Pareto principle appears to be suitable for the OCTAVE^{SM} viewpoint. As deep as the context of information security, such an interesting principle can be interpreted 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 center's resources (i.e. time, budget, personnel, etc.) on these areas, optimum fruit is achieved in a limited amount of time, whilst the effort involved is simultaneously reduced as a positive by-product of this approach.

- ***Capturing the 'Organizational view on information security' – A challenge for large-scale and dispersed organization***

Indeed, if we look into the way to conduct from Process 1 to 3, we'll see how complicated and vast the data collected are, especially in a large-scale and dispersed organization. The larger and more hierarchical the organization, the more challenging it is for gathering, consolidating and analyzing these data. Therefore, without the assistance of strong data processing and analyzing software tools, hardly can a risk assessment provide a reliable result.

- ***Open communication – A paradoxically-seeming challenge***

One of the most important risk management principles of the OCTAVE is quite challenging to implement. In risk evaluation, people freely discuss sensitive information about what is not working well in an organization and how the organization's critical assets are at risk. Understandably, in many organizations, such a free exchange of information might, according to few senior management, be a way to put the organization out of business. Moreover, as far as I have observed, people are prone to keeping issues to themselves if they are in the workshop with someone to whom they report. Consequently, the more hierarchical the organization, the less chance this principle can be successfully adopted. Therefore, OCTAVE^{SM} suggests that there be no reporting relationship among the people in a workshop and that there be a culture that supports open communication.

- ***Threat Profiles – A challenge of assessing the risk in overall relationship***

The benefits of using Threat Profiles to analyze risk are unarguable. However, it seems that, in the OCTAVE^{SM}, the interrelations among risks occurring to information assets are not mentioned when conducting the analysis of risk impact on the organization. Let's take this study as an example with some assumptions. Indeed, if I could put all the created Threat Profiles in only paper and connect them together in the order (e.g. in terms of asset, access, actor, motive, etc.), I would wonder that if an attacker physically intruded into the center to:

(1) destroy some NCs (assuming that this threat results in a 'low EV' and 'Acceptance approach'),

(2) access and modify the UIPS via the network (assuming that this threat also results in 'low EV' and 'Acceptance approach'), and

(3) view management data (assuming that this threat also results in 'low EV' and 'Acceptance approach'),

then how the OCTAVE^{SM} would assess the EV in this circumstance.

Obviously, if each incident occurs separately, there's nothing to discuss the EV result. The problem is that when combining three incidents that simultaneously happen, the total Expected Value of the organization (e.g. by adding three 'Low EV' together) may not be 'Low EV' anymore and certainly, the approach is not the risk acceptance. Though the above assumed situation does not happen in this study, I find it safer and more appropriate to put all Threat Profiles in a one space (if conveniently) so that assessor can make decisions more accurate. Personally, this is a weakness of the OCTAVE^{SM}, which should be improved in the near future.

- ***Dealing with probability in information security***

Perhaps, this will continue being one of the hottest and knottiest issues for security experts in many years. Solution to work out this issue, in my opinion, could be either seeking a new definition of 'Expected Loss' equation using a new dimension instead of subjective probability or strengthening and devising the tools and methods that can relatively accurately and completely observe the statistical information regarding information security breaches and incidents. Only then can the risk assessment results be more reliable.

- ***Risk assessment can not be a 'silver bullet'***

Last but not least, it's worth mentioning that not all the risks assessed as 'High EV' can be mitigated or controlled. Such examples are the risk of 'Internet connection shutdown' in the Risk Profile of system problems for NCs and 'Lack of sufficient budget' in the Risk Profile of other problems for technical team. Simply, these risks are out of control of the center.

2.2 Information Security Management System Based on BS and ISO Standards

2.2.1 Advantages

- There is a close relationship between the ISMS and QMS (ISO 9000 series) or EMS (ISO 14001) in terms of structure and requirements. Thus, if an organization has already implemented QMS, it would be easy and convenient to implement an additional ISMS. On the other hand, unlike QMS or EMS, the risk assessment, in particular and risk management, in general plays the key role in establishing an efficient ISMS. This is understandable because the core of information security is dealing with the risk issues. Understanding this fact, organizations would find it less complicated and more motivative to follow the system's requirements.

- Since the processes of ISMS are based on the PDCA approach, it would be more possible to succeed than other approaches to ISMS. For decades, the truth of Deming's philosophy has been observed throughout the industries.

- The six-step of establishing ISMS follows a 'top-down' approach. It starts with senior management from a managerial perspective and ends with selecting control objectives from a technical perspective. This substantially reflects the viewpoint of many academic and practitioners on information security: "Security is a management issue not a technology issue".

- ISMS based on BS 7799 and ISO 17799 is quite flexible. Organizations can justify the standards to make the ISMS suitable to their own specific context. This is particularly significant since I find it hard to justify the model if organizations choose to follow other approaches to ISMS.

- Step 5 - Selection of controls in establishing ISMS is worth mentioning. It enables to solve the identified levels of risks more systematically than other approaches. For example, rather than benchmarking with widely recognized best practices, other approaches just lay emphasis on ready-to-use practices. This way puts the ISMS in an inefficient posture when solving risk problems.

2.2.2 Weakness

The only problem that I have perceived so far is also the statement at the beginning of ISO 17799:2000 Bulletin – additional controls may be required. Since the ISO/IEC 17799 is actually an adoption of the original BS 7799:1-1999, a few controls appear not to cover new evolution of IT in recent years. Such an illustration is the insufficiency or lack of controls for wireless network access whose threats are more and more alarming or for e-transactions over Internet, which are increasingly diversified, sophisticated and easily vulnerable to many hackers. More discussion about these issues of technological changes will be in the very next section.

2.2.3 Other problems - Trade-Offs: Security, privacy, technological innovation, and costs

Selecting controls and writing policies in this fast-changing advanced technological area require balancing a number of essential trades-offs:

Security and Costs. Security controls should be qualitatively proportional to the real value of the information assets. Given this argument, it appears that when the information asset value is small, no clear risk management case can be made for employing the most sophisticated security measures when a less expensive form of security will yield the same return. For instance, in this study, if users (i.e. students, lecturers) register for protecting some of their important data, management would save costs for buying less backup data storage.

Security and Technological Innovation. The impressive proliferation of information technology in recent year brings us a coin with two sides. The right side is that organizations can benefit from the IT evolution is enhancing their security management system whilst the left side offers information criminals more chances to attack organization's information assets. Consequently, management could feel reluctant to adopt standards or guidelines, insisting that policies may not worth return on investment. In this case, I would absolutely agree with various academics and practitioners that security standards should be sufficiently flexible and technology-neutral.

Security and Privacy/Culture. Paradoxically, the need for more effective security controls may sometimes conflict with and negatively affect staff' and user's privacy. This issue, in my opinion, is not new but full of controversies. On the one hand, certain types of security policies may be consistent with protecting privacy (e.g. using programs such as scanning email content). On the other hand, it may be needed to track and verify staff' and user's movements. Thus, in my opinion, writing policies should also be accompanied by proper balancing between security and privacy, in particular and the cultural aspects, in general. For example, in this study, the Thai context, policy on the disciplinary process for staff who accidentally violate security regulations can not be the same with those applied in Western countries. Care should also be taken for governmental laws and regulations.

3. SOME COMMENTS AFTER THIS THESIS WORK

Although my intention in this thesis work is merely taking the ECC as a specific case study, it's interesting to see a few improvements in terms of security practices such as:

- ➢ directly inputting the print quota into the UIPS – this is important since in the past students should bring the paper of print quota to the technical team. They themselves can change the content of this paper,
- ➢ enhancing physical security for the server rooms,
- ➢ enhancing physical security for accessing to the center.

4. SUGGESTION FOR FUTURE STUDY

The ISMS based on BS 7799 and ISO 17799 could facilitate for future studies on:

- ➢ Establishing ISMS based on the Information Security Management Standards fitting the Thai context. Australia and New Zealand, India, Japan, Germany are those who have developed their own standards adapted from the ISO 17799: 2000.
- ➢ Information security risk assessment using the OCTAVE^{SM} method for large-scale, dispersed organizations in Thailand.

"Sure, the firm had a firewall to protect and filter, but it was all wide open to anyone with an 802.11(x) card".
Simson Garfinkle, Co-founder, Sandstorm Enterprises

5. FINAL CONCLUSION

Simson, co-founder of Sandstorm Enterprises, may be reasonable with his ironical remark if we consider it from a managerial perspective. Indeed, here and there, it's tempting that many organizations are chasing up the latest technological security measures without laying stress on their organizational policies. Once they do not dedicate their resources right to the core of information security, suffering failures are understandable and inevitable.

There goes a good saying, "Let's policy drives technology, procedures and testing". Therefore, I would think that the decision to establish ISMS based on the two standards is a proper way to materialize that truth.

I found it interesting to close this study with the two news for those who have successfully established the ISMS – the good and bad.

The good news is that from now on, they can effectively secure their information assets as well as ensure business continuity. The bad news is that they'll never be at the end of the journey called *'controlling information security risks'.* Such a particular work is endless.