REFERENCES

1. WSOIS Bulletin. (December 2003). WSOIS: Geneva, Switzerland.
2. AFP News Singapore. (October 2003). *"Forecast: Asia to upgrade IT Security"*. Business – Bangkok Post.
3. AP News Belgium. (November 2003). *"EU On Guard"*. Database – Bangkok Post.
4. Boonruang Sasiwimon. (27 August 2003). *"Security specialist sets up rep office here"*. Database – Bangkok Post.
5. Karnjanatawe Karnjana. (26 March 2003). *"Govt unites on security - Standard details 10 security areas"*. Database: Bangkok Post.
6. Kevin D. Mitnick. (2003). *"The Art of Deception: Controlling the human element of security"*. New York: O'reilly & Associates, Inc.
7. Raymond R. Panko. (2003). "Network Security: A beginner's Guide". New Jersey: Addision – Wesley.
8. Alberts Christopher and Dorofee Audrey. (2003). Managing Information Security Risks – The Octave[SM] Approach. Boston: Addision – Wesley.
9. Garfinkel Simson, Spafford Gene. (2002). Web Security, Privacy & Commerce, 2nd ed. CA: O'reilly & Associates, Inc.
10. Boonruang Sasiwimon. (October 2003). Local bank's online services 'exposed'. Database – Bangkok Post.
11. Pfleeger P. Charles, Pfleeger Lawrence Shari. (2003). Security in Computing, 3rd ed. Upper Saddle River, NJ: Pearson Education International.
12. Ferdinand Pamela and Barbaro Michael. (26 July 2002). *"Yale Tells FBI of Rival's Breach of Web Site"*. Washington Post.
13. Ferdinand Pamela and Barbaro Michael. (30 July 2002). *"Princeton's network hack investigation"*. Washington Post.
14. Vigilinx. (April 2001). *"White Paper: Security Assessment Methodology"*. URL:http://www.vigilinx.com.
15. ISO/IEC 17799:2000 – Information Technology: Code of Practice for information security management, 1st edition.
16. Szomanski B. (2001). "Integracja systemu zarzadzania bezpieczenstwem infomracji zgodnie z BS7799 z zintegrowanymi systemami zarzadzania (ISO 9001, ISO 14001, PN 18000).". Enigma 2001. URL:http://www.bezpieczenstwoIT.pl
17. Stonebrunner, Gary, Alice Goguen, and Alexis Feringa. (October 2001). *"Risk Management Guide for Information Technology Systems"*. NIST Special, Publication 800-30, URL:http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
18. ISO IEC/TR 13335-3:1998 - Information technology - Guidelines for the management of IT Security: Part 3: Techniques for the management of IT Security.
19. Thow-Chang Lim, Siew-Mun Kwan and Foo Alvin. (2002). *"Information Security Management Systems and Standards"*. Sun Professional Services, Thailand.
20. Visintine Vishal. (August 8, 2003). *"An Introduction to Information Risk Assessment"*. GSEC Practical, Version 1.4b. SANS Institute.
21. Ding Tan. (December 2002). *"Quantitative Risk Analysis Step-By-Step"*. SANS Institute.

22. Jedynak A. (13 October 2000). *"Newest Microsoft technologies: Microsoft Solution Framework"*. Conference Roadshow: Warsaw, Finland.
23. Robert, Jacobson. (15 August, 2002). *"Quantifying IT Risks"*. ITAudit. URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=479.
24. Fites P.E., Kratz M.P. and Brener A.F. (1989). *"Control and Security of Computer Information Systems"*. Rockville, MD: Computer Science Press.
25. United States General Accounting Office. (November 1999). *"Information Security Risk Management, Practices of leading organizations (GAO/AIMD-00-03"*. Washington, DC: GAO.
26. Thomas Finne. (1996). *"Analyzing Information Security: Knowledge-Based DSS Approach"*. Abo Akademi University, Institute for Advanced Management Systems Research: Finland.
27. Chapman, C.B. (1991). *"Risk in investment, procurement and performance in construction"*. E&F Spon.
28. Department of Defense. (1985). *"Trusted Computer System Evaluation Criteria (TCSEC)."*.
29. Schell R.R. and Brinkley D.L. (1995). *"Evaluation Criteria for Trusted Systems"* cited from Abrams M. D., Jajoda S. and Podell H.J. (1995). *"Information Security – an Integrated Collection of Essays"*. IEEE Computer Society Press: Los Alamitos, California, pp. 137-160.
30. Clark David & David Wilson. (1987). Proceedings. IEEE USA.
31. ITSEC (28 June 1991). Information Technology Security Evaluation Criteria. Commission of European Communities.
32. WMG. (2003). Module Note – Quality Management & Techniques. Coventry: WMG.
33. Gullep Eralp. (13/20 May 2003). *"How to implement information security"*. Bangkok Post-Database. Global Risk Management Solutions, PricewaterhouseCoopers, Thailand.
34. Coffee Peter, Duck Timothy, Sturdevant Cameron, Rapoza Jim. (2003). *"5 Weeks to Enterprise Security"*. An EWEEK Whitepaper.
35. BS 7799:2-2002 - Information security management: Specifications with guidance for use.

Website:

36. URL:http://www.infoworld.com/News,
37. URL:http://www.cert.org
38. URL:http://www.standford.edu/itss/news
39. URL:http://www.mit.edu/cpnews;
40. URL:http://www.zone-h.org
41 URL:http://www.sans.org
42. URL: http://www.ist-usa.com/aboutcora.htm
43. URL:http://www.security-risk-analysis.com/introduction.htm
44. URL:http://www.riskworld.net/advantages.htm
45. URL:http://www.peltierassociates.com/frap.htm
46. URL:http://www.securityforum.org/ReportsLibrary2002/categories/cat/risk.htm
47. URL:http://www.cve.mitre.org
48. URL:http://www.tqmi.com/nl/is.pdf

49 URL:http://stqc.nic.in/itservices/overview.htm
50 URL:http://www.eweek.com
51. URL:http://www.bsi-global.com
52. URL:http://www.callio.com/page.asp?id=85
53. URL:http://www.nectec.or.th/ThaiCERT

BIBLIOGRAPHY

1. Von Solms E. - University of South Africa, Prof Eloff J.H.P - Rand Afrikaans University (2002). "Information Security Development Trends". http://osprey.unisa.ac.za/saicsit2001/Electronic/paper52.PDF
2. Marcel Dekker. (1997). *"Security of the Internet"*. The Froehlich/Kent Encyclopedia of Telecommunications, vol.15, New York: pp.231-255.
3. Dorothy E. Deming. (1999). Information Warefare and Security. Reading, Massachusetts: Addition Wesley, Inc.
4. Hutt Arthur E., Bosworth Seymour and Hoyt Douglass B. (1995). Computer Security Handbook. New York: John Willley & Sons, Inc.
5. Caelli William, Longley Dennis and Shain Michael. (1991). Information Security Handbook. New York: Stockton Press.
6. Van Scoy, Roger L. (September 1992). *"Software Development Risk: Opportunity, Not Problem. Software"*. Software Engineering Institute, CMU/SEI-92-TR-30, ADA 258743, Carnegie Mellon University.
7. Thomas Glaessner, Tom Kellermann, Valerie McNevin. (June 2002). "Electronic Security: Risk Mitigation in Financial Transactions - Public Policy Issues". http://www.isalliance.org/resources/papers/E-security.pdf
8. Archie D. Andrews Jr. (March 23, 2003). "Security Program Management and Risk". GIAC Security Essentials Certification Practical Assignment Version 1.4b. © SANS Institute.
9. Ian Rathie. (2002). "An Approach to Application Security". SANS Security Essentials. SANS Institute.
10. Unknown Author. (accessed 6 August 2003). "Features". C & A Systems Security. URL:http://www.riskworld.net/advantages.htm.
11. Unknown Author. (accessed 6 August 2003). "ISO 17799". C & A Systems Security. URL:http://www.riskworld.net/7799.htm.
12. Peltier, Thomas. (accessed 6 August 2003). "Peltier Associates Facilitated Risk Analysis Process (FRAP).". URL:http://www.peltierassociates.com/frap.htm.
13. Unknown author. (June 2002). "Information Risk Management". Information Security Forum.. URL:http://www.securityforum.org/ReportsLibrary2002/categories/cat/risk.htm, accessed 6 August 2003.
14. Unknown Author. "Introduction to Risk Analysis". C & A Systems Security. URL:http://www.security-risk-analysis.com/introduction.htm, accessed 6 Aug. 2003.
15. The Oxford Advanced English Learner's Dictionary (2003).

Websites

16. URL:http://www.rsa.com
17. URL:http://www.gammassl.co.uk/bs7799/history.html
18. URL:http://www.isosecuritysolutions.com/standardmain.html
19. URL:http://www.aba-dialogue.org/
20. URL:http://www.issa.org/

APPENDIX A

APPENDIX A-0

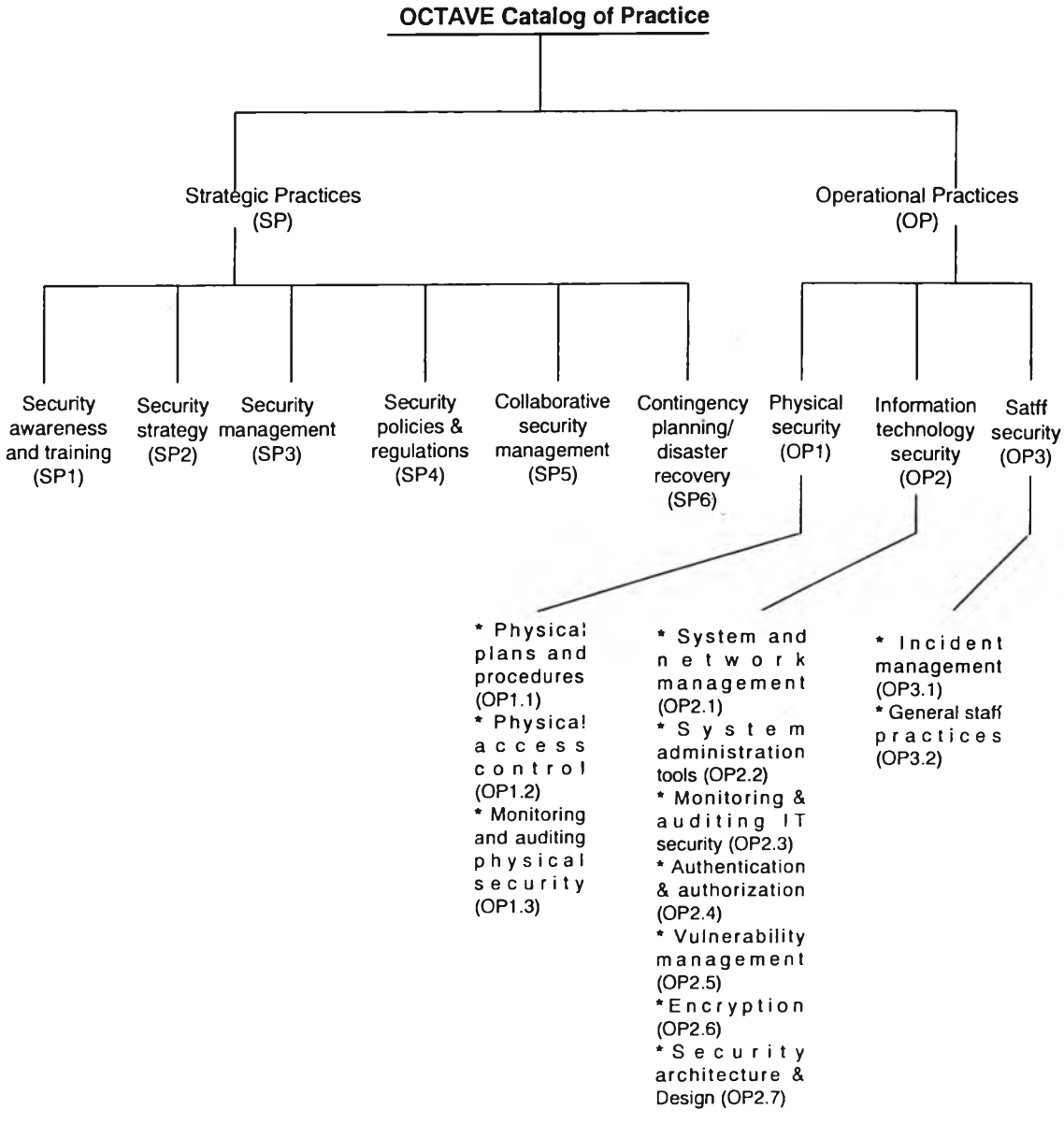

FIGURE A-0: *Structure of the OCTAVE[SM] Catalog of Practices*

Source: *Christopher and Audrey (2003), p.444.*

STRATEGIC PRACTICES *Security Awareness and Training - SP1*	
SP1.1	Staff members understand their security roles and responsibilities. This is documented and verified.
SP1.2	There is adequate in-house expertise for all supported services, mechanism and technologies (e.g. logging, monitoring or encryption), including their security operation. This is documented and verified.
SP1.3	Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified. Training includes these topics: • Security strategies, goals and objectives. • Security regulations, policies and procedures. • Policies and procedures for working with third parties. • Contingency and disaster recovery plans. • Physical security requirements. • Users' perspective on: - system and network management - system administration tools - monitoring and auditing for physical and information technology security - authentication and authorization - vulnerability management - architecture and design Incident management General staff practices Enforcement, sanctions and disciplinary actions for security violations How to properly access sensitive information or work in areas where sensitive information is accessible Termination policies and procedures relative to security

STRATEGIC PRACTICES *Security Strategy – SP2*	
SP2.1	The organization's business strategies routinely incorporate security considerations
SP2.2	Security strategies and policies take into consideration the organization's business strategies and goals
SP2.3	Security strategies, goals and objectives are documented and are routinely reviewed, updated and communicated to the organization

STRATEGIC PRACTICES *Security Management – SP3*	
SP3.1	Management allocates sufficient funds and resources to information security activities
SP3.2	Security roles and responsibilities are defined for all staff in the organization
SP3.3	The organization's hiring and termination practices for staff take information security issues into account
SP3.4	The required levels of information security and how they are applied to individuals and groups are documented and enforced.
SP3.5	The organization manages information security risks, including: • Assessing risks to information security both periodically and in response to major changes in technology, internal/external threats or the organization's systems and operations • Taking steps to mitigate risks to an acceptable level • Maintaining an acceptable level of risk • Using information security risk assessment to help select cost-effective security/control measures, balancing implementation costs against potential losses
SP3.6	Management receives and acts upon routine reports summarizing the results of • Review of system logs • Review of audit trails • Technology vulnerability assessment • Security incidents and the responses to them • Risk assessments • Physical security review • Security improvement plans and recommendations

STRATEGIC PRACTICES *Security Policies and Regulations – SP4*	
SP4.1	The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated. These policies address key security topic areas, including: • Security strategy and management • Security risk management • Physical security • System and network management • System administration tools • Monitoring and auditing • Authentication and authorization • Vulnerability management • Encryption • Security architecture and design • Incident management • Staff security practices • Applicable laws and regulations • Awareness and training • Collaborative information security • Contingency planning and disaster recovery
SP4.2	There is a documented process for management of security policies, including: • Creation • Administration (including periodic reviews and updates) • Communication
SP4.3	The organization has a documented process for periodic evaluation (technical and nontechnical) of compliance with information security policies, applicable laws and regulations and insurance requirements.
SP4.4	The organization has a documented process to ensure compliance with information security policies, applicable laws and regulations and insurance requirements.
SP4.5	The organization uniformly enforces its security policies
SP4.6	Testing and revision of security policies and procedures are restricted to authorized personnel.

STRATEGIC PRACTICES *Collaborative Security Management – SP5*	
SP5.1	The organization has documented, monitored and enforced procedures for protecting its information when working with external organizations (e.g. third parties, collaborators, subcontractors or partners)
SP5.2	The organization has verified that outsourced security services, mechanisms and technologies meet its needs and requirements.
SP5.3	The organization documents, monitors and enforces protection strategies for information belonging to external organizations that is accessed from its own infrastructure components or is used by its own personnel.
SP5.4	The organization provides and verifies awareness and training on applicable external organization's security policies and procedures for personnel who are involved with those external organizations.
SP5.5	There are documented procedures for terminated external personnel specifying appropriate security measures for ending their access. These procedures are communicated and coordinated with the external organization.

STRATEGIC PRACTICES *Contingency Planning/Disaster Recovery – SP6*	
SP6.1	An analysis of operations, applications and data criticality has been performed.
SP6.2	The organization has documented • Business continuity or emergency operation plans • Disaster recovery plan(s) • Contingency plan(s) for responding to emergencies
SP6.3	The contingency, disaster recovery and business continuity plans consider physical and electronic access requirements and controls.
SP6.4	The contingency, disaster recovery and business continuity plans are periodically reviewed, tested and revised.
SP6.5	All staff • Are aware of the contingency, disaster recovery and business continuity plans • Understand and are able to carry out their responsibilities.

OPERATIONAL PRACTICES *Physical Security – OP1* *Physical Security Plans and Procedures – OP1.1*	
OP1.1.1	There are documented facility plan(s) for safeguarding the premises, buildings and any restricted areas.
OP1.1.2	These plans are periodically reviewed, tested and updated.
OP1.1.3	Physical security procedures and mechanisms are routinely tested and revised.
OP1.1.4	There are documented policies and procedures for managing visitors, including • Sign-in • Escort • Access logs • Reception and hosting
OP1.1.5	There are documented policies and procedures for physical control of hardware and software, including Workstations, laptops, modems, wireless components and all other components used to access information. Access, storage and retrieval of data backups. Storage of sensitive information on physical and electronic media Disposal of sensitive information or the media on which it is stored. Reuse and recycling of paper and electronic media.

OPERATIONAL PRACTICES *Physical Security – OP1* *Physical Access Control – OP1.2*	
OP1.2.1	There are documented policies and procedures for individual and group access covering • The rules for granting the appropriate level of physical access • The rules for setting an initial right of access • Modifying the right of access • Terminating the right of access • Periodically reviewing and verifying the rights of access
OP1.2.2	There are documented policies. procedures and mechanism for controlling physical access to defined entities. This includes • Work areas • Hardware (computers, communication devices, etc.) and software media
OP1.2.3	There are documented procedures for verifying access authorization prior to granting physical access.

OP1.2.4	Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.

OPERATIONAL PRACTICES *Physical Security – OP1* *Monitoring and Auditing Physical Security – OP1.3*	
OP1.3.1	Maintenance records are kept to document the repairs and modifications of a facility's physical components.
OP1.3.2	An individual's or group's actions, with respect to all physically controlled media, can be accounted for.
OP1.3.3	Audit and monitoring records are routinely examined for anomalies and corrective action is taken as needed.

OPERATIONAL PRACTICES *Information Technology Security – OP2* *System and Network Management – OP2.1*	
OP2.1.1	There are documented security plan(s) for safeguarding the systems and networks
OP2.1.2	Security plan(s) are periodically reviewed, tested and updated
OP2.1.3	Sensitive information is protected by secure storage, such as • Defined chains of custody • Backups stored off-site • Removable storage media • Discard process for sensitive information or its storage media
OP2.1.4	The integrity of installed software is regularly verified.
OP2.1.5	All systems are up to date with respect to revisions, patches and recommendation in security advisories.
OP2.1.6	There is a documented data backup plan that • is routinely updated • is periodically tested • calls for regularly scheduled backups of both software and data • requires periodic testing and verification of the ability to restore from backups
OP2.1.7	All staff understand and are able to carry out their responsibilities under the backup plans
OP2.1.8	Changes to IT hardware and software are planned, controlled and documented.

OP2.1.9	IT staff members follow procedures when issuing, changing and terminating users' passwords, accounts and privileges. • Unique user identification is required for all information system users, including third-party users • Default accounts and default passwords have been removed from systems
OP2.1.10	Only necessary services are running on systems; all necessary services have been removed

OPERATIONAL PRACTICES *Information Technology Security – OP2* *System Administration Tools – OP2.2*	
OP2.2.1	New security tools, procedures and mechanisms are routinely reviewed for applicability in meeting the organization's security strategies
OP2.2.2	Tools and mechanisms for secure system and network administration are used and are routinely reviewed and updated or replaced. Examples are: • Data integrity checkers • Cryptographic tools • Vulnerability scanners • Password-quality-checking tools • Virus scanners • Process management tools • Intrusion detection systems • Secure remote administrations • Network service tools • Traffic analyzers • Incident response tools • Forensic tools for data analysis

OPERATIONAL PRACTICES *Information Technology Security – OP2* *Monitoring and Auditing IT Security – OP2.3*	
OP2.3.1	System and network monitoring and auditing tools are routinely used by the organization. • Activity is monitored by the IT staff • System and network activity is logged/recorded • Logs are reviewed on regular basis • Unusual activity is dealt with according to the appropriate policy or procedure • Tools are periodically reviewed and updated.
OP2.3.2	Firewall and other security components are periodically audited for compliance with policy.

OPERATIONAL PRACTICES *Information Technology Security – OP2* *Authentication and Authorization – OP2.4*	
OP2.4.1	Appropriate access controls and user authentication (e.g. file transmission, network configuration) consistent with policy are used to restrict user access to • Information • System utilities • Program source code • Sensitive systems • Specification applications and services • Network connections within the organization • Network connections from outside the organization
OP2.4.2	There are documented information-use policies and procedures for individual and group access to • Establish the rules for granting the appropriate level of access • Establish an initial right of access • Modify the right of access • Terminate the right of access • Periodically review and verify the rights of access
OP2.4.3	Access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.
OP2.4.4	Access control methods/mechanisms are periodically reviewed and verified.

OP2.4.5	Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered or destroyed in an unauthorized manner.
OP2.4.6	Authentication mechanisms are used to protect availability, integrity and confidentiality of sensitive information. Examples are: • Digital signatures • Biometrics

OPERATIONAL PRACTICES *Information Technology Security – OP2* *Vulnerability Management – OP2.5*	
OP2.5.1	There is a documented set of procedures for managing vulnerability, including: • Selecting vulnerability evaluation tools, checklists and script • Keeping up to date with known vulnerability types and attack methods • Reviewing sources of information on vulnerability announcements, security alerts and notices • Identifying infrastructure components to be evaluated • Scheduling of vulnerability evaluations • Interpreting and responding to the results • Maintaining secure storage and disposition of vulnerability data
OP2.5.2	Vulnerability management procedures are followed and are periodically reviewed and updated.
OP2.5.3	Technology vulnerability assessments are performed on a periodic basis and vulnerabilities are addressed when they are identified.

OPERATIONAL PRACTICES *Information Technology Security – OP2* *Encryption – OP2.6*	
OP2.6.1	Appropriate security controls are used to protect sensitive information while in storage and during transmissions, including • Data encryption during transmission • Data encryption when writing to disk • Use of public key infrastructure • Virtual private network technology • Encryption for all Internet-based transmission
OP2.6.2	Encrypted protocols are used when remotely managing systems, routers and firewalls
OP2.6.3	Encryption controls and protocols are routinely reviewed, verified and revised.

OPERATIONAL PRACTICES *Information Technology Security – OP2* *Security Architecture and Design – OP2.7*	
OP2.7.1	System architecture and design for new and revised systems include considerations for • Security strategies, policies and procedures • History of security compromises • Results of security risk assessments
OP2.7.2	The organization has up-to-date diagrams that show the enterprisewide security architecture and network topology.

OPERATIONAL PRACTICES *Staff Security – OP3* *Incident Management – OP3.1*	
OP3.1.1	Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations, including • Network-based incidents • Physical access incidents • Social engineering incidents
OP3.1.2	Incident management procedures are periodically tested, verified and updated.
OP3.1.3	There are documented policies and procedures for working with law enforcement agencies.

OPERATIONAL PRACTICES *Staff Security – OP3* *General Staff Practices – OP3.2*	
OP3.1.1	Staff members follow good security practices, such as: • Securing information for which they are responsible • Not divulging sensitive information to others (resistant to social engineering) • Having adequate ability to use information technology hardware and software • Using good password practices • Understanding and following security policies and regulations • Recognizing and reporting incidents
OP3.1.2	All staff at all levels of responsibility implement their assigned roles and responsibility for information security.
OP3.1.3	There are documented procedures for authorizing and overseeing those who work with sensitive information or who work in locations where the information resides. This includes: Employees Contractors, partners, collaborators and personnel from third-party organizations System maintenance personnel Facilities maintenance personnel

APPENDIX A-1

Asset Worksheet

1. What are your important assets? Consider the following:
   - Information: academic data, users' data, paper personnel records, financial data, management data, contract data.
   - System: email system, computing system, user information processing system (UIPS).
   - Software: application software.
   - Hardware: personal computers (desktops & laptops), network and networking components (servers, routers, switches, hubs and optical fibers), network protection components (Firewall, Intrusion Detection System –IDS, Intrusion Prevention System – IPS, Virtual Private Network – VPN).
   - People: technical team.
2. Are there any other assets that you are required to protect (e.g. by law or regulation)? N/A
3. What related assets are important? Consider the following:
   - Information
   - System
   - Software
   - Hardware
   - People
4. From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?

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 great importance 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 CHULANET.	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.

APPENDIX A-2

Areas of Concern Worksheet

What scenarios threaten your important assets?

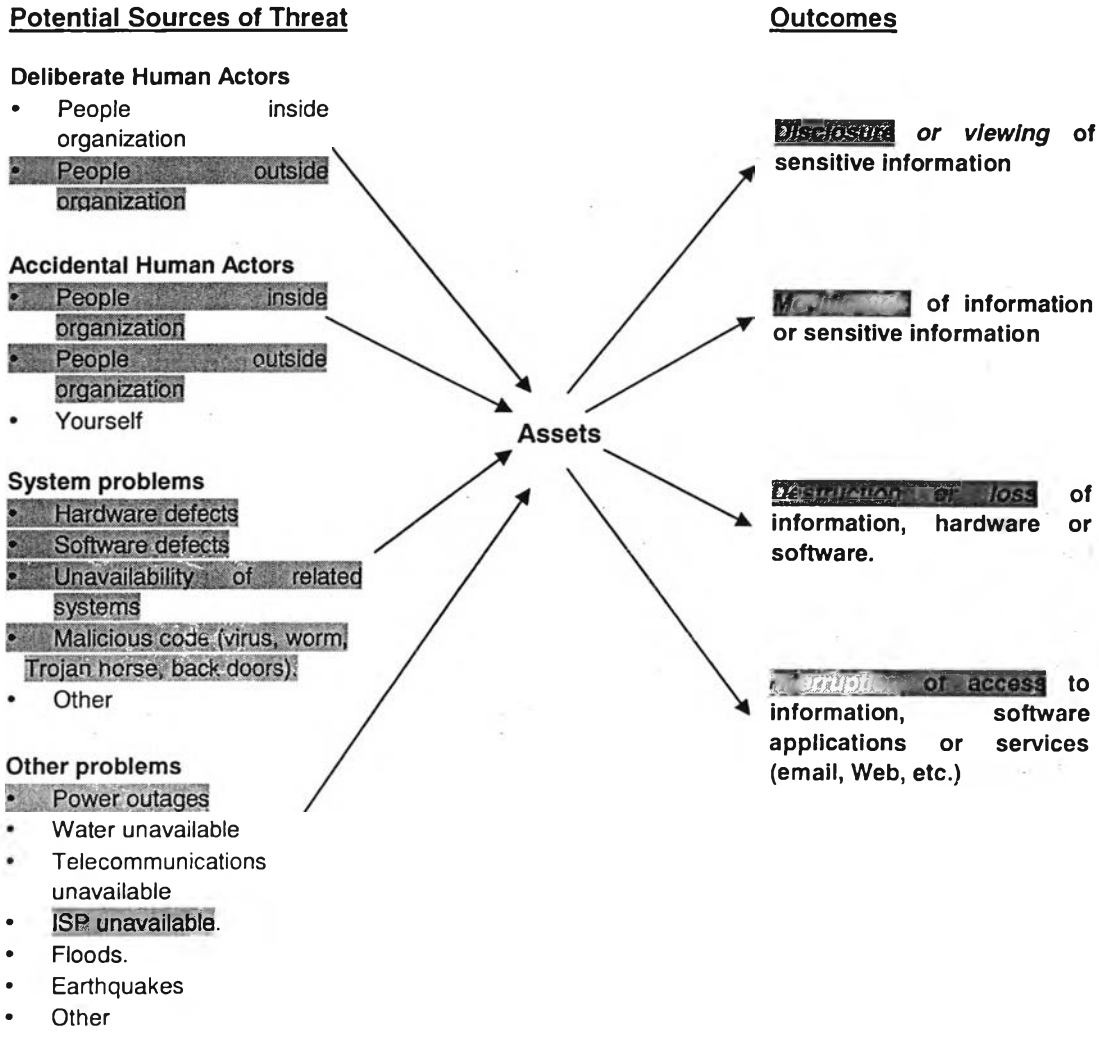

TABLE A-2.1: *Threat Sources*

Adapted from TABLE 5-4, p. 95, Christopher and Audrey (2003).

Category of Threat Source	Definition
Deliberate actions by people	This group includes people inside and outside the center who might take deliberate action against the information assets
Accidental actions by people	This group includes people inside and outside the center who might accidentally harm the information assets
System problems	These are problems with information technology systems. Examples include hardware defects, software defects, unavailability of related systems, viruses, malicious codes and other system-related problems.
Other problems	These problems are beyond the center's control. Threats in this category include natural disasters (e.g. floods, earthquakes) that can effect the center's information technology systems, unavailability of systems maintained by other organizations, and interdependency issues, which include problems with infrastructure services, such as power outages, broken water pipes and telecommunication.

TABLE A-2.2: *Threat Outcomes*

Adapted from TABLE 5-5, p. 95, Christopher and Audrey (2003).

Threat outcome	Definition
Disclosure	The viewing of confidential or proprietary information by someone who should not see the information
Modification	An authorized changing of an asset
Loss/Destruction	The limiting of an asset's availability, either temporarily or because it is unrecoverable
Interruption	Th limiting of an asset's availability, mainly in terms of services

APPENDIX A-3

Security Requirement Worksheet
5. What are the important security requirements for each information asset? Consider the following: • Confidentiality: Users' data (**); UIPS (**); PCs (*); NCs(*); • Integrity: Users' data (***); UIPS (*); PCs (**); NCs(**); • Availability: Users' data (*); UIPS (***); PCs (***); NCs(***); Technician team (***) • Other: NA *Note: '***' means highly important; '**' means moderately important; '*' means lowly important.*
6. What is the relative ranking of the security requirements for each information asset? Which security requirement is the most important? Relative ranking of security requirements for each information asset is also included in question 1. Details on priority and specific requirements are provided in the table below.

TABLE A-3.1: *Security Requirement Worksheet*

Security Requirement Worksheet			
Security Requirement Type		*Priority*	*Specific Requirement*
Confidentiality	Users' data		Users' data should be kept confidential for privacy. Only authorized persons can access to these data for some particular reasons.
	Management data	x	Management data must be kept confidential. Any unauthorized actions must be identified and prevented immediately.
	UIPS		UIPS should be kept confidential. Those who are not in charge of running the system should be strictly prevented from accessing it.
	PCs		
	NCs		Some NCs should be kept confidential due to their value and importance to other functions. Any unauthorized actions must be identified and prevented actively and timely.
	Technical Team		
Integrity	Users' data	x	Users' data must be maintained accurate and complete. Due care must be spent on any unauthorized actions that aim at modifying or destroying such data.
	Management data		Like users' data, management data should also be maintained accurate and complete. Attention should be paid to those who try to access without official permission and observation.
	UIPS	x	UIPS, PCs and NCs should be kept in good condition. Attention should be paid to any unauthorized persons whose purpose is to modify or destroy the logical and physical configurations of the system.
	PCs		
	NCs		
	Technician Team		

Availability	Users' data		Access to users' data as well as management data should be ensured 24/7. It must be available for the needs of study, communication and daily management.
	Management data		
	UIPS		UIPS, PCs and NCs must be ensured to be in good condition at any time. Special attention should be paid to any logical and physical damages that occur to them.
	PCs	x	
	NCs	x	
	Technician Team	x	Technician team must be available 24/7 to make sure the continuity and the good performance of the entire information system at ECC.

APPENDIX A-4

B.1.4.1 Senior Management Survey

Name (optional):

Position: Head of ECC

Senior Management Survey			
Practice	*Is this practice used by your organization?*		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes x	No	Don't know
There is adequate in-house expertise for all supported services, mechanism and technologies (e.g. logging, monitoring or encryption), including their secure operation. This is documented and verified.	Yes x	No	Don't know
Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No x	Don't know
Security Strategy			
The organization's business strategies routinely incorporate security considerations.	Yes	No x	Don't know
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes x	No	Don't know
Security strategies, goals and objectives are documented and are routinely reviewed, updated and communicated to the organization.	Yes	No x	Don't know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No x	Don't know
Security roles and responsibilities are defined for all staff in the organization.	Yes x	No	Don't know

The organization's hiring and termination practices for staff take information security issues into account.	Yes x	No	Don't know
The organization manages information security risks by assessing existing risks to information security and taking steps to mitigate information security risks.	Yes x	No	Don't know
Management receives and acts upon routine reports summarizing security-related information (e.g. audits, logs, risk and vulnerability assessments).	Yes	No x	Don't know
Security Polices and Regulations			
The organization has a complete set of documented, current policies that are periodically reviewed and updated.	Yes	No x	Don't know
There is a documented process for management of security policies: 1. Creation 2. Administration (including periodic review and updates) 3. Communication	Yes x	No	Don't know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations and insurance requirements.	Yes	No x	Don't know
The organization uniformly enforces its security policies.	Yes x	No	Don't know
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g. third parties, collaborators, subcontractors or partners): 1. Protecting information belonging to other organizations. 2. Understanding the security polices and procedures of external organization. 3. Ending access to information by terminated external personnel.	Yes	No x	Don't know
The organization has verified that outsourced security services, mechanism and technologies meet its needs and requirements.	Yes X	No	Don't know

Contingency Planning/Disaster Recovery			
An analysis of operation, applications and data criticality has been performed.	Yes	No x	Don't know
The organization has documented, reviewed and tested business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Yes	No x	Don't know
The contingency, disaster recovery and business continuity plans consider physical and electronic access requirements and controls.	Yes x	No	Don't know
All staff are aware of the contingency, disaster recovery and business continuity plans and understand and are able to carry out their responsibilities.	Yes	No	Don't know x
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings and any restricted areas are documented and tested.	Yes	No x	Don't know
There are documented policies and procedures for managing visitors.	Yes	No x	Don't know
There are documented policies and procedures for physical control of hardware and software.	Yes x	No	Don't know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes x	No	Don't know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes x	No	Don't know
System and Network Management			
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes x	No	Don't know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans	Yes x	No	Don't know

Authentication and Authorization			
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes x	No	Don't know
Incident Management			
Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations.	Yes x	No	Don't know
Incidents management procedures are periodically tested, verified and updated.	Yes	No x	Don't know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No x	Don't know
General Staff Practices			
Staff members follow security practice, for example: • Securing information for which they are responsible • Not divulging sensitive information to others (resistance to social engineering) • Ensuring they have adequate ability to use information technology hardware and software • Using good password practices • Understanding and following security policies and regulations • Recognizing and reporting incidents	Yes x	No	Don't know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes x	No	Don't know
There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.	Yes x	No	Don't know

B.1.4.2 Operational Area Management Survey

Name (optional):

Position: Heads of technical division and administration division.

Operational Area Management Survey			
Practice	*Is this practice used by your organization?*		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes x	No	Don't know
There is adequate in-house expertise for all supported services, mechanism and technologies (e.g. logging, monitoring or encryption), including their secure operation. This is documented and verified.	Yes x	No	Don't know
Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No x	Don't know
Security Strategy			
The organization's business strategies routinely incorporate security considerations.	Yes	No x	Don't know
Security strategies and polices take into consideration the organization's business strategies and goals.	Yes x	No	Don't know
Security strategies, goals and objectives are documented and are routinely reviewed, updated and communicated to the organization.	Yes	No x	Don't know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No x	Don't know
Security roles and responsibilities are defined for all staff in the organization.	Yes x	No	Don't know
The organization's hiring and termination practices for staff take information security issues into account.	Yes x	No	Don't know

The organization manages information security risks by assessing to information security and taking steps to mitigate information security risks.	Yes	No x	Don't know
Management receives and acts upon routine reports summarizing security-related information (e.g. audits, logs, risk and vulnerability assessment).	Yes	No x	Don't know
Security Policies and Regulations			
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes	No x	Don't know
There is a documented process for management of security policies: 1. Creation 2. Administration (including periodic review and updates) 3. Communication	Yes x	No	Don't know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations and insurance requirements.	Yes	No x	Don't know
The organization uniformly enforces its security policies.	Yes x	No	Don't know
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g. third parties, collaborators, subcontractors or partners): 1. Protecting information belonging to other organizations. 2. Understanding the security polices and procedures of external organization. 3. Ending access to information by terminated external personnel.	Yes	No x	Don't know
The organization has verified that outsourced security services, mechanism and technologies meet its needs and requirements.	Yes	No X	Don't know

Contingency Planning/Disaster Recovery			
An analysis of operation, applications and data criticality has been performed.	Yes	No x	Don't know
The organization has documented, reviewed and tested business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Yes	No x	Don't know
The contingency, disaster recovery and business continuity plans consider physical and electronic access requirements and controls.	Yes x	No	Don't know
All staff are aware of the contingency, disaster recovery and business continuity plans and understand and are able to carry out their responsibilities.	Yes x	No	Don't know
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings and any restricted areas are documented and tested.	Yes	No x	Don't know
There are documented policies and procedures for managing visitors.	Yes	No x	Don't know
There are documented policies and procedures for physical control of hardware and software.	Yes x	No	Don't know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes x	No	Don't know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes x	No	Don't know
Monitoring and Auditing Physical Security			
Audit and monitoring records are routinely examined for anomalies and corrective action is taken as needed.	Yes	No x	Don't know

System and Network Management			
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes x	No	Don't know
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans	Yes	No	Don't know x
Authentication and Authorization			
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes x	No	Don't know
Incident Management			
Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations.	Yes x	No	Don't know
Incident management procedures are periodically tested, verified and updated.	Yes	No x	Don't know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No x	Don't know
General Staff Practices			
Staff members follow security practice, for example: • Securing information for which they are responsible • Not divulging sensitive information to others (resistance to social engineering) • Ensuring they have adequate ability to use information technology hardware and software • Using good password practices • Understanding and following security policies and regulations • Recognizing and reporting incidents	Yes x	No	Don't know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	No	Don't know x
There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.	Yes x	No	Don't know

B.1.4.3 General Staff Survey

Name (optional):

Position: Admin staff

General Staff Survey:			
Practice	*Is this practice used by your organization?*		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes x	No	Don't know
There is adequate in-house expertise for all supported services, mechanism and technologies (e.g. logging, monitoring or encryption), including their secure operation. This is documented and verified.	Yes	No	Don't know x
Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No x	Don't know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No x	Don't know
Security roles and responsibilities are defined for all staff in the organization.	Yes x	No	Don't know
The organization's hiring and termination practices for staff take information security issues into account.	Yes x	No	Don't know
The organization manages information security risks by assessing risks to information security and taking steps to mitigate information security risks.	Yes	No x	Don't know

Security Policies and Regulations			
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Yes	No x	Don't know
There is a documented process for management of security policies: 1. Creation 2. Administration (including periodic review and updates) 3. Communication	Yes x	No	Don't know
The organization uniformly enforces its security policies.	Yes x	No	Don't know
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g. third parties, collaborators, subcontractors or partners): 1. Protecting information belonging to other organizations. 2. Understanding the security polices and procedures of external organization. 3. Ending access to information by terminated external personnel.	Yes	No	Don't know x
Contingency Planning/Disaster Recovery			
All staff are aware of the contingency, disaster recovery and business continuity plans and understand and are able to carry out their responsibilities.	Yes	No	Don't know x
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings and any restricted areas are documented and tested.	Yes	No x	Don't know
There are documented policies and procedures for managing visitors.	Yes	No x	Don't know
There are documented policies and procedures for physical control of hardware and software.	Yes x	No	Don't know

Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes x	No	Don't know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes x	No	Don't know
System and Network Management			
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans	Yes	No	Don't know x
Incident Management			
Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations.	Yes x	No	Don't know
Incident management procedures are periodically tested, verified and updated.	Yes	No x	Don't know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No	Don't know x
General Staff Practices			
Staff members follow security practice, for example: • Securing information for which they are responsible • Not divulging sensitive information to others (resistance to social engineering) • Ensuring they have adequate ability to use information technology hardware and software • Using good password practices • Understanding and following security policies and regulations • Recognizing and reporting incidents	Yes x	No	Don't know
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes x	No	Don't know
There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.	Yes x	No	Don't know

B.1.4.4 IT Staff Survey

Name (optional):

Position: Technical staff

IT Staff Survey			
Practice	*Is this practice used by your organization?*		
Security Awareness and Training			
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes x	No	Don't know
There is adequate in-house expertise for all supported services, mechanism and technologies (e.g. logging, monitoring or encryption), including their secure operation. This is documented and verified.	Yes x	No	Don't know
Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Yes	No x	Don't know
Security Strategy			
The organization's business strategies routinely incorporate security considerations.	Yes	No x	Don't know
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes x	No	Don't know
Security strategies, goals and objectives are documented and are routinely reviewed, updated and communicated to the organization.	Yes	No x	Don't know
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No x	Don't know
Security roles and responsibilities are defined for all staff in the organization.	Yes x	No	Don't know
The organization's hiring and termination practices for staff take information security issues into account.	Yes x	No	Don't know

The organization manages information security risks by assessing existing risks to information security and taking steps to mitigate information security risks.	Yes x	No	Don't know
Management receives and acts upon routine reports summarizing security-related information (e.g. audits, logs, risk and vulnerability assessments).	Yes	No X	Don't know
Security Polices and Regulations			
The organization has a complete set of documented, current policies that are periodically reviewed and updated.	Yes	No x	Don't know
There is a documented process for management of security policies: 1. Creation 2. Administration (including periodic review and updates) 3. Communication	Yes x	No	Don't know
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations and insurance requirements.	Yes	No	Don't know x
The organization uniformly enforces its security policies.	Yes x	No	Don't know
Collaborative Security Management			
The organization has policies and procedures for protecting information when working with external organizations (e.g. third parties, collaborators, subcontractors or partners): 1. Protecting information belonging to other organizations. 2. Understanding the security polices and procedures of external organization. 3. Ending access to information by terminated external personnel.	Yes	No x	Don't know
The organization has verified that outsourced security services, mechanism and technologies meet its needs and requirements.	Yes x	No	Don't know

Contingency Planning/Disaster Recovery			
An analysis of operation, applications and data criticality has been performed.	Yes	No x	Don't know
The organization has documented, reviewed and tested business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	Yes	No x	Don't know
The contingency, disaster recovery and business continuity plans consider physical and electronic access requirements and controls.	Yes x	No	Don't know
All staff are aware of the contingency, disaster recovery and business continuity plans and understand and are able to carry out their responsibilities.	Yes	No x	Don't know
Physical Security Plans and Procedures			
Facility security plans and procedures for safeguarding the premises, buildings and any restricted areas are documented and tested.	Yes	No x	Don't know
There are documented policies and procedures for managing visitors.	Yes	No x	Don't know
There are documented policies and procedures for physical control of hardware and software.	Yes x	No	Don't know
Physical Access Control			
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes x	No	Don't know
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes x	No	Don't know
Monitoring and Auditing Physical Security			
Maintenance records are kept to document the repairs and modifications of a facility's physical components.	Yes x	No	Don't know
An individual's or group's actions with respect to all physically controlled media can be accounted for.	Yes	No	Don't know x

Audit and monitoring records are routinely examined for anomalies and corrective action is taken as needed.	Yes	No x	Don't know
System and Network Management			
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes x	No	Don't know
Sensitive information is protected by secure storage (e.g. backups stored off-site, discard process for sensitive information)	Yes x	No	Don't know
The integrity of installed software is regularly verified.	Yes x	No	Don't know
All systems are up to date with respect to revisions, patches and recommendations in security advisories.	Yes	No	Don't know x
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Yes x	No	Don't know
Changes to IT hardware and software are planned, controlled and documented.	Yes x	No	Don't know
IT staff members follow procedures when issuing, changing and terminating users' passwords, accounts and privileges: • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.	Yes x	No	Don't know
Only necessary services are running on systems; all unnecessary services have been removed.	Yes x	No	Don't know
System Administration Tools			
Tools and mechanisms for secure system and network administration are used and they are routinely reviewed and updated or replaced.	Yes x	No	Don't know

Monitoring and Auditing IT Security			
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.	Yes x	No	Don't know
Firewall and other security components are periodically audited for compliance with policy.	Yes x	No	Don't know
Authentication and Authorization			
Appropriate access controls and user authentication (e.g. file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services and network connections.	Yes x	No	Don't know
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes x	No	Don't know
Methods or mechanism are provided to ensure that sensitive information has not been accessed, altered or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.	Yes x	No	Don't know
Vulnerability Management			
There is a document set of procedures for managing vulnerabilities: • Selecting vulnerability evaluation tools, checklists and scripts • Keeping up to date with known vulnerability types and attack methods • Reviewing sources of information on vulnerability announcements, security alerts and notices • Identifying infrastructure components to be evaluated • Scheduling of vulnerability evaluations • Interpreting and responding to the results • Maintaining secure storage and disposition of vulnerability data	Yes	No x	Don't know
Vulnerability management procedures are followed and are periodically reviewed and updated.	Yes x	No	Don't know
Technology vulnerability assessments are performed on a periodic basis and vulnerabilities are addressed when they are identified.	Yes x	No	Don't know

Encryption			
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g. data encryption, public key infrastructure, virtual private network technology).	Yes x	No	Don't know
Encrypted protocols are used for remote management of systems, routers and firewalls.	Yes x	No	Don't know
Security Architecture and Design			
System architecture and design for new and revised systems include considerations for: • Security strategies, policies and procedures • History of security compromises • Results of security risk assessments	Yes	No x	Don't know
The organization has up-to-date diagrams that show the enterprisewide security architecture and network topology.	Yes	No	Don't know x
Incident Management			
Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations.	Yes x	No	Don't know
Incident management procedures are periodically tested, verified and updated.	Yes	No x	Don't know
There are documented policies and procedures for working with law enforcement agencies.	Yes	No	Don't know x
General Staff Practices			
Staff members follow security practice, for example: • Securing information for which they are responsible • Not divulging sensitive information to others (resistance to social engineering) • Ensuring they have adequate ability to use information technology hardware and software • Using good password practices • Understanding and following security policies and regulations • Recognizing and reporting incidents	Yes x	No	Don't know

All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes x	No	Don't know
There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.	Yes x	No	Don't know

APPENDIX A-5

Current Strategic Practices of ECC

TABLE A-5.1: *Security Awareness & Training*

Security Awareness and Training				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Staff members understand their security roles and responsibilities. This is documented and verified.	Yes	Yes	Yes	Yes
There is adequate in-house expertise for all supported services, mechanism and technologies (e.g. logging, monitoring or encryption), including their secure operation. This is documented and verified.	Yes	Yes	Unclear	Yes
Security awareness, training and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	No	No	No	No

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management	We have a clear statement of the center containing rules and regulations for working.	Staff, in general and IT staff, in particular are not regularly and formally provided with up-to-date knowledge of security management. They just learn by themselves.
Operational area management	Necessary skills and expertise for maintaining the operation are also available.	General staff's security awareness is not good enough. They just can respond to "familiar" incidents or signs.

General staff	We strictly follow the rules and regulations set up by the center.	We do not know whether we can effectively and timely respond to unexpected and unknown incidents. Hopefully, the technology and skills that the center possesses is enough.
IT staff		Awareness training is inadequate.

TABLE A-5.2: *Security Strategy*

Security Strategy				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
The organization's business strategies routinely incorporate security considerations.	No	No		No
Security strategies and policies take into consideration the organization's business strategies and goals.	Yes	Yes		Yes
Security strategies, goals and objectives are documented and are routinely reviewed, updated and communicated to the organization.	No	No		No

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		Strictly speaking, we should pay much attention to security by regularly including it into our operation strategies.
Operational area management		Current protection strategies need to be enhanced more remarkably.
General staff		We do not clearly understand how security strategies link to the operation strategies of the center.
IT staff		It's best to spend more time discussing in-depth the new security strategies.

TABLE A-5.3: *Security Management*

Security Management				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Management allocates sufficient funds and resources to information security activities.	No	No	No	No
Security roles and responsibilities are defined for all staff in the organization.	Yes	Yes	Yes	Yes
The organization's hiring and termination practices for staff take information security issues into account.	Yes	Yes	Yes	Yes
The organization manages information security risks by assessing existing risks to information security and taking steps to mitigate information security risks.	Yes	No	No	Yes
Management receives and acts upon routine reports summarizing security related information (e.g. audits, logs, risk and vulnerability assessments).	No	Unclear		No

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management	We carry out vulnerability scan very often. Results obtained are used for enhancing security strategies.	I don't think we actually get those kind of reports; Maybe we should
Operational area management	It's good that we have included security requirements into the working contract when recruiting personnel at the center.	I'm concerned about the complacency or ignorance. Sometimes, I think we are lucky.
General staff		
IT staff		Budget is not enough for enhancing security measures. We need more advanced tools to support the security strategies.

TABLE A-5.4: *Security Policies & Regulations*

Security Policies and Regulations				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
The organization has a complete set of documented, current policies that are periodically reviewed and updated.	No	No	No	No
There is a documented process for management of security policies: 4. Creation 5. Administration (including periodic review and updates) 6. Communication	Yes	Yes	Yes	Yes
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations and insurance requirements.	No	No		Unclear
The organization uniformly enforces its security policies.	Yes	Yes	Yes	Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management	Policies and procedures do exist. We require that all staff, before starting their work, read the security policies and regulations.	A documented process for ensuring compliance with information security policies is not prepared. We think it's also necessary.
Operational area management		
General staff	We strictly follow security policies and rules. That's our duty.	
IT staff		Security policies and regulations are rarely updated. Only techniques and tools are our primary concerns.

TABLE A-5.5: *Collaborative Security Management*

Collaborative Security Management				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
The organization has policies and procedures for protecting information when working with external organizations (e.g. third parties, collaborators, subcontractors or partners): 4. Protecting information belonging to other organizations. 5. Understanding the security polices and procedures of external organization. 6. Ending access to information by terminated external personnel.	No	No	Unclear	No
The organization has verified that outsourced security services, mechanism and technologies meet its needs and requirements.	Yes	No		Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		In the past, we have no relations with external organizations except for some organizations in the university. We should consider this issue once we want to expand our relationship with third-parties. This is very important.
Operational area management	We check whether security services (i.e. some free downloadable vulnerability testing software) meet our needs and requirements.	
General staff		We do not see such requirements in the common security policies and regulations.
IT staff		

***TABLE A-5.6:* Contingency Planning/Disaster Recovery**

Contingency Planning/Disaster Recovery				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
An analysis of operation, applications and data criticality has been performed.	No	No		No
The organization has documented, reviewed and tested business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies.	No	No		No
The contingency, disaster recovery and business continuity plans consider physical and electronic access requirements and controls.	Yes	Yes		Yes
All staff are aware of the contingency, disaster recovery and business continuity plans and understand and are able to carry out their responsibilities.	Unclear	Yes	Unclear	No

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		We do not have an effective disaster recovery plan except for some general but not specific guidelines.
Operational area management	Our business continuity plans also mention about physical and electronic access requirements. This control is crucial to our activities.	That's a good idea to perform an analysis of our operation and identify a link between our activities and data criticality. We did not do before.
General staff		All we know about contingency is just fire. We think its meaning is broader than it really is.
IT staff		Contingency and emergency plans should be clearer and realistic. We see so many general guidelines but find it hard to implement in this complex IT environment.

Current Operational Practices of ECC:

TABLE A-5.7: Physical Security Plan & Procedures

Physical Security Plans and Procedures: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Facility security plans and procedures for safeguarding the premises, buildings and any restricted areas are documented and tested.	No	No	No	No
There are documented policies and procedures for managing visitors.	No	No	No	No
There are documented policies and procedures for physical control of hardware and software.	Yes	Yes	Yes	Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		I'm not sure how often the plans and procedures are tested.
Operational area management		We should also mention about managing visitors such as staff' friends or relatives in sensitive areas.
General staff		There is little challenging of people after working hours.
IT staff	Documented policies to control physical access to hardware and software are quite sufficient and in accordance with the center's rules and regulations.	

TABLE A-5.8: *Physical Access Control*

Physical Access Control: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes	Yes	Yes	Yes
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes	Yes	Yes	Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		We could reallocate the printing room to another place. It's very close to the server's room.
General staff	We are required to lock up our offices and PCs carefully and have a quick check up our computing facilities at the end of the day.	Physical security is hampered by: - Location/distribution of terminals - Large and decentralized computing facilities. - Shared codes to cipher locks.
IT staff	Hardware especially networking security is good	

TABLE A-5.9: *Monitoring & Auditing Physical Security*

Monitoring and Auditing Physical Security: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Maintenance records are kept to document the repairs and modifications of a facility's physical components.				Yes
An individual's or group's actions with respect to all physically controlled media can be accounted for.				Unclear
Audit and monitoring records are routinely examined for anomalies and corrective action is taken as needed.		No		No

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		I think the technical team does not audit and monitor very often. They just do this at the year-end when we have to submit technical reports to the faculty.
General staff		
IT staff		We just track repairs and modifications. We think it's hard to control whether an individual's or group's actions are in accordance with physically controlled media or not.

TABLE A-5.10: *System & Network Management*

System and Network Management: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes	Yes		Yes
Sensitive information is protected by secure storage (e.g. backups stored off-site, discard process for sensitive information)				Yes
The integrity of installed software is regularly verified.				Yes
All systems are up to date with respect to revisions, patches and recommendations in security advisories.				Unclear
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans	Yes	Unclear	Unclear	Yes
Changes to IT hardware and software are planned, controlled and documented.				Yes
IT staff members follow procedures when issuing, changing and terminating users' passwords, accounts and privileges: • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.				Yes
Only necessary services are running on systems; all unnecessary services have been removed.				Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management	We surely have a specific security plan. It is developed mainly by the technical team.	The effectiveness of security plans and procedures is rarely tested in reality. Serious incidents could reveal whether they are good or not.
Operational area management		I'm not sure the people outside IT understand they have those responsibilities.
General staff		
IT staff	- We know what we're supposed to do. - Systems are well protected with passwords, authorizations, etc. We force our users to change their passwords. - We care about the source, stability and completeness of the installed application software. - We strictly limit the number of services as well as application running on our system. Only those that are crucial and popular are taken into consideration.	- We just make backups for our management data not users' data. - We think we cannot catch up with all latest security-related information everyday. We only focus on highlighted and well-known incidents reported on Internet. - We think we do not clean up inherited access rights quite well. We should pay more attention to this problem.

TABLE A-5.11: *System Administration Tools*

System Administration Tools: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Tools and mechanisms for secure system and network administration are used and they are routinely reviewed and updated or replaced.				Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		
General staff		
IT staff	The technical team is in charge of all such activities. They keep their eyes on the system as well as reports on incidents on Internet.	Technical team cannot have sufficient up-to-date system administration tools. More investment should be spent on security protection tools.

TABLE A-5.12: *Monitoring & Auditing IT Security*

Monitoring and Auditing IT Security: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.				Yes
Firewall and other security components are periodically audited for compliance with policy.				No

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		
General staff		
IT staff	It's the main duty of the technical team to do all audits and run monitoring tools. They particularly pay attention to unusual signs occurring to the system.	

TABLE A-5.13: *Authentication & Authorization*

Authentication and Authorization: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Appropriate access controls and user authentication (e.g. file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services and network connections.				Yes
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	Yes		Yes
Methods or mechanism are provided to ensure that sensitive information has not been accessed, altered or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.				Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management	There are policies for access control and permissions.	
General staff		
IT staff	Systems are well protected with passwords, authorizations, etc.	We cannot guarantee that we are 100% exempted from new attacks. We need to increase our protection level more and more.

TABLE A-5.14: *Authentication & Authorization*

Vulnerability Management: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
There is a document set of procedures for managing vulnerabilities: • Selecting vulnerability evaluation tools, checklists and scripts • Keeping up to date with known vulnerability types and attack methods • Reviewing sources of information on vulnerability announcements, security alerts and notices • Identifying infrastructure components to be evaluated • Scheduling of vulnerability evaluations • Interpreting and responding to the results • Maintaining secure storage and disposition of vulnerability data				No
Vulnerability management procedures are followed and are periodically reviewed and updated.				Yes
Technology vulnerability assessments are performed on a periodic basis and vulnerabilities are addressed when they are identified.				Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		
General staff		

IT staff	- We perform vulnerability scanning on the regular basis and when we think it's could be under danger according to suggestion and reports. - What we deal with information security is to keep in track with reported security-related announcements and alerts and then decide.	- We do not have as many as vulnerability tools to select. What we have been doing is to utilize what is either prevalent or suggested by and available in the community. - We never discuss and communicate the sources of information on vulnerabilities.

TABLE A-5.15: *Encryption*

Encryption: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g. data encryption, public key infrastructure, virtual private network technology).				Yes
Encrypted protocols are used for remote management of systems, routers and firewalls.				Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		
General staff		
IT staff		- Hopefully, we could implement IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) soon. - Currently, all we can do is implement a good encryption and firewall. Yet, we think it's not enough in the future, if we do not have VPN (virtual private network).

TABLE A-5.16: *Security Architecture & Design*

Security Architecture and Design: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
System architecture and design for new and revised systems include considerations for: • Security strategies, policies and procedures • History of security compromises • Results of security risk assessments				No
The organization has up-to-date diagrams that show the enterprisewide security architecture and network topology.				Unclear

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		
Operational area management		
General staff		
IT staff		- We rarely take into account history of all components and especially previous risk assessment when upgrading the system. - Diagrams or network topology are just redrawn when there are basic and important changes but no minor changes.

TABLE A-5.17: *Incident Management*

Incident Management: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations.	Yes	Yes	Yes	Yes
Incident management procedures are periodically tested, verified and updated.	No	No	No	No
There are documented policies and procedures for working with law enforcement agencies.	No	No	Unclear	Unclear

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management		- Our center belongs to the faculty that's within the university. All we care about is to follow the faculty's and university's rules and regulations only. So far, we have never concerned with any other law enforcement. - We're mainly concerned with how to respond with some incidents such as fire, stealing or virus. We do not have specific procedures for management this issue.
Operational area management	We do have instructions on incident respond.	Not everyone is aware of the procedures.
General staff	We are regularly reminded of strictly keeping an eye on information-security breaches	
IT staff		Dealing with law enforcement should be the work of either the faculty of engineering or the university.

TABLE A-5.18: General Staff Practices

General Staff Practices: Survey results				
Survey Statement	*Senior Managers*	*Operational Area Managers*	*General staff*	*IT Staff*
Staff members follow security practice, for example: • Securing information for which they are responsible • Not divulging sensitive information to others (resistance to social engineering) • Ensuring they have adequate ability to use information technology hardware and software • Using good password practices • Understanding and following security policies and regulations • Recognizing and reporting incidents	Yes	Yes	Yes	Yes
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Yes	Unclear	Yes	Yes
There are documented procedures for authorizing and overseeing all staff (including personnel from third party organizations) who work with sensitive information or who work in locations where the information resides.	Yes	Yes	Yes	Yes

Comments		
Organizational Level	*Protection Strategy Practices*	*Organizational Vulnerabilities*
Senior management	Implementing security practices is an indispensable part of hiring and termination' contract.	
Operational area management		Not all staff implement roles and responsibilities especially those outside IT. This might attribute to their lack of IT knowledge.
General staff		
IT staff	We pay due care to those who work in sensitive areas.	

APPENDIX A-6

Users' data		
Threat type	*Areas of concern*	*Threat Properties*
Human actors using network access (including wireless network)	Due to carelessness or unintention, when working on users' data, IT staff personnel could damage or modify users' data via accessing networks (i.e. misconfigurations and other administration errors).	Asset – Users' data Access – Network Actor – insiders Motive – accidental Outcome - modification, loss/destruction, interruption.
	Purposefully, some people outside the ECC (i.e. disgruntled students, external organizations, etc.) attempt to intrude into the network to access users' data and then do unauthorized actions. Outsiders can utilize either some software tools or social engineering to intrude into the data system and do unauthorized activities.	Asset – Users' data Access – Network Actor – outsiders Motive – deliberate Outcome - modification, disclosure, loss/destruction, interruption.
	Some students, when leaving the computers unattended, did not log off or lock their accounts. Other students may unintentionally or carelessly modify, damage or cause interruption.	Asset – Users' data Access – Network Actor – outsiders Motive – accidental Outcome - modification, loss/destruction, interruption.
System problems	Data after being created and processed are stored in hard disks. Due to some application software defects (i.e. run-time errors, miscofiguration or missing files, etc.), data can be modified or incomplete or accessing to data can be inaccessible.	Asset – Users' data Actor – Software defects Outcome - modification, loss/destruction, interruption.
	Hardware defects can damage the data storage in terms of modification, loss or destruction or inaccessibility.	Asset – Users' data Actor – Hardware defects Outcome - modification, loss/destruction, interruption.

System problems	Many types of application-level attacks, both new and old, (i.e. exploitable URLs, worms, Trojan-horses and virus) are the primary concerns to data storage and transmission.	Asset – Users' data Actor – Malicious codes/programs Outcome - modification, disclosure, loss/destruction, interruption.
	According to previous experiences, user ID & password management appear not to be highly effective. With some advanced technological tools and techniques (i.e. keytrokes), intruders may hack into users' data after lots of attempts.	Asset – Users' data Actor – Weak authentication Outcome - modification, disclosure, loss/destruction, interruption.
Other problems	Instability or interruption of power supply system are the causes of logical loss/destruction of the data or of inaccessibility to the data.	Asset – Users' data Actor – Power supply system Outcome – modification, loss/destruction, interruption.
	Technical team is sometimes very busy. Team must support other divisions in university. Technical team may not recognize the importance of users' data or may lack continuos due care for the users' data.	Asset – Users' data Actor – Technical team not available Outcome - interruption.

Management data		
Threat type	*Areas of concern*	*Threat Properties*
Human actors using network access (including wireless network)	Due to carelessness or unintention, IT and general staff personnel could damage management data via accessing network (i.e. misconfigurations and other administration errors).	Asset – Management data Access – Network Actor – insiders Motive – accidental Outcome - modification, loss/destruction, interruption.
	Some staff, when leaving the 'data management interface' unattended, may let outsiders (i.e. visitors) unintentionally perform actions without permittance.	Asset – Management data Access – Network Actor – outsiders Motive – accidental Outcome - modification, loss/destruction, interruption.
	Purposefully, some people outside the ECC (i.e. disgruntled students, external organizations, etc.) attempt to intrude into the network to access management data for their own objectives. For instance, social engineering is a preferable technique for many hackers to intrude into the data system.	Asset – Management data Access – Network Actor – outsiders Motive – deliberate Outcome - modification, disclosure, loss/destruction, interruption.
System problems	Management data after being created and processed are stored in hard disks. Due to some application software defects (i.e. run-time errors, miscofiguration or missing files, etc.), data can be modified or incomplete or accessing to data can be inaccessible.	Asset – Management data Actor – Software defects Outcome - modification, loss/destruction, interruption.
	Hardware defects can damage the data storage in terms of modification, loss or destruction or inaccessibility.	Asset – Management data Actor – Hardware defects Outcome - modification, loss/destruction, interruption.
	Many types of application-level attacks, both new and old, (i.e. exploitable URLs, worms, Trojan-horses and virus) are the primary concerns to data storage and transmission.	Asset – Management data Actor – Malicious codes/programs Outcome - modification, disclosure, loss/destruction, interruption.

	There are two problems to be concerned. First, a high number of general and IT staff personnel have access to management data. Second, management data are often stored in an easily readable plaintext format. Stored in a software environment and exposed in such a manner, data are vulnerable to discovery.	Asset – Management data Actor – Accessing and storing mismanagement Outcome - modification, disclosure, loss/destruction.

UIPS		
Threat type	*Areas of concern*	*Threat Properties*
Human actors using network access (including wireless network)	There are a few problems to be concerned: - Some IT staff may enter the wrong data, resulting in incorrect individual records (i.e. privileges, services or print quota, etc.). - A high number of IT staff have access to much information. Role-based access builds over time and replacements inherit all of those access privileges. Thus, they might accidentally lose, modify or damage part of users' data. - Communication about users' information (i.e. privileges, services or print quota, etc.) between general staff and IT staff or among IT staff themselves is in an insecure manner.	Asset – UIPS Access – Network Actor – insiders Motive – accidental Outcome – modification, loss/destruction, interruption.
	People outside ECC can accidentally affect the operation of the system via network access (e.g. they could unknowingly send emails infected with malicious codes or programs to the system).	Asset – UIPS Access – Network Actor – outsiders Motive – accidental Outcome – modification, loss/destruction, interruption.
	Outsiders (i.e. disgruntled students, staff and external organizations) may deploy advanced techniques and tools to affect the system through the network for their adverse purposes (i.e. bomb email, spam mail, malicious codes/program, denial-of-service attacks).	Asset – UIPS Access – Network Actor – outsiders Motive – deliberate Outcome – modification, disclosure, loss/destruction, interruption.
System problem	The UIPS might be interrupted, modified or destroyed (e.g. inaccessibility to the email system) due to the defects of some application software building up the entire UIPS such as run-time errors, operating system errors, incompatibility among system components or versions during upgrading or maintaining, etc.	Asset – UIPS Actor – Application/system software defects. Outcome - modification, loss/destruction, interruption.

	The UIPS might crash or its processed information might be lost or modified due to the problem of hardware defects such as servers or PCs crash, instable performance of LAN (Local Area Network), etc..	Asset – UIPS Actor – Hardware defects. Outcome - modification, loss/destruction, interruption.
	UIPS could be infected with malicious codes/programs that could distribute individual or sensitive information such as emails and messages, cause inaccessibility to email system and modify or destroy important users' administration information.	Asset – UIPS Actor – Malicious codes/programs. Outcome – disclosure, interruption, loss/destruction, modification.
Other problem	Instability or interruption of power supply system are the causes of logical loss/destruction of the UIPS or of denial of access to the UIPS. This essentially shuts the ECC's operation down.	Asset – UIPS Actor – Power supply system Outcome – modification, loss/destruction, interruption.
	Technical team cannot continuously pay due care to the UIPS because they occasionally support other divisions in the faculty of engineering when necessary.	Asset – UIPS Actor – Technical team availability Outcome – interruption.

PCs		
Threat type	*Areas of concern*	*Threat Properties*
Human actors using physical access	Staff personnel might unintentionally or carelessly damage the PC's physical configuration.	Asset – PCs Access – physical access Actor – insiders Motive – accidental Outcome – modification, loss/destruction, interruption.
	Outsiders may unintentionally or carelessly damage the PC's physical configuration. Previous experiences revealed that few students are not highly aware of keeping and maintaining PC in good condition.	Asset – PCs Access – physical access Actor – outsiders Motive – accidental Outcome – modification, loss/destruction, interruption.
	Outsiders (i.e. disgruntled students, staff or external organizations) could directly damage the PC's physical configuration or directly view the information on the PC screen. Without proper controlling, the aftermath is severe.	Asset – PCs Access – physical access Actor – outsiders Motive – deliberate Outcome – modification, disclosure, loss/destruction, interruption.
System problems	Any internal or external components of the PC could crash, leaving it unstable or failed to run. A high frequency of working hours increases such a risk of failure of these components.	Asset – PCs Actor – Hardware defects Outcome - modification, loss/destruction, interruption.
	PCs are easily and directly vulnerable to many malicious codes/programs (viruses, Trojan horses, worms). Once infected with these elements, they cannot either perform correctly or shut down. In some cases, individual or sensitive information can be modified or exposed to public.	Asset – PCs Actor – Malicious codes/programs Outcome - modification, loss/destruction, disclosure, interruption.
	Some PCs and components, when they are in need of substitution, either wait for a long time to be done or are left unrepaired. The budget for buying new components or PCs is very limited.	Asset – PCs Actor – Unavailability of PC's components for substitution Outcome - loss/destruction, interruption.

	Individual or sensitive information stored on shared network drives can be exposed to the public.	Asset – PCs Actor – Shared network drives Outcome – disclosure.
Other problems	Instability or interruption of power supply system can cause logical or physical loss/destruction of or inaccessibility to the PCs.	Asset – PCs Actor – Power supply system Outcome - loss/destruction, interruption.
	Fire or thunder would cause severe damages in terms of loss/destruction of PC's physical configuration or inaccessibility to the PC.	Asset – PCs Actor – Fire, thunder, flood, explosion, magnetic force Outcome – modification, loss/destruction, interruption.
	There are currently 130 out of 321 computers being used at ECC. Clearly speaking, five IT staff are not sufficient to keep and maintain a wide range of computing facilities in good condition continuously.	Asset – PCs Actor – Unavailability of technical team support Outcome - interruption.

NCs		
Threat type	*Areas of concern*	*Threat Properties*
	IT Staff personnel might unintentionally or carelessly affect the NC's logical configuration.	Asset – NCs Access – network access Actor – insiders Motive – accidental Outcome – modification, interruption, loss/destruction
Human actors using network access (including wireless network)	Outsiders might unintentionally modify, interrupt or damage network components or network performance in terms of logical configuration.	Asset – NCs Access – network access Actor – outsiders Motive – accidental Outcome – modification, interruption, loss/destruction.
	Outsiders (i.e. disgruntled students, staff or external organizations) may intrude from an intermediate, remote workstation connecting with ECC's Network and perform unauthorized actions such as modifying NC's logical configuration, stealing and distributing sensitive information regarding network administration, etc. Serious consequences are network system crashes, denial-of-services of routers, switches and Web servers, etc.	Asset – NCs Access – network access Actor – outsiders Motive – deliberate Outcome – modification, interruption, loss/destruction, disclosure.
Human actors using physical access	Staff personnel might unintentionally or carelessly damage the NC's physical configuration.	Asset – NCs Access – physical access Actor – insiders Motive – accidental Outcome – modification, interruption, loss/destruction.

	Outsiders (i.e. students, lecturers or visitors) may unintentionally or carelessly damage the NC's physical configuration. For example, hubs for each computer room are improperly and insecurely located. Thus, the risk of physical vulnerability is apparent.	Asset – NCs Access – physical access Actor – outsiders Motive – accidental Outcome – modification, interruption, loss/destruction
	Outsiders (i.e. disgruntled students, staff or external organizations) could directly damage the NC's physical configuration. The more knowledgeable they are about the NCs, the more severe consequences they cause. The room where web servers, routers and switches are located are adjacent to the printing room (which is freely accessible) and are not strictly protected from unauthorized persons.	Asset – NCs Access – physical access Actor – outsiders Motive – deliberate Outcome – modification, interruption, loss/destruction.
	If components of the Network crash, Network performance will be unstable. Some NCs can be damaged during operating.	Asset – NCs Actor – Hardware defects Outcome - loss/destruction, interruption.
System problem	NCs require lots of application/network administration software to be run. Therefore, if one of those failed to activate/start, Network performance would experience interruption, modification or loss of administration data. Exemplified problems are run-time errors, network administration system errors, incompatibility among network application software or software versions during upgrading (e.g. installing security patches from vendors) or maintaining, etc.	Asset – NCs Actor – Application/network administration software defects Outcome - modification, loss/destruction, interruption.

	NCs are easily and directly vulnerable to many malicious codes/programs (viruses, Trojan horses, worms). Once infected with these elements, they cannot either perform correctly or shut down. In some cases, sensitive or network administration system-related information can be modified or exposed to public.	Asset – NCs Actor – Malicious codes/programs Outcome - modification, disclosure, loss/destruction, interruption.
	ECC's Network could not perform to its highest capability once the CHULANET web servers were down. As a result, data transmission between ECC's Network with external organizations collapses.	Asset – NCs Actor – Internet (CUNET Web server malfunctioned) connection shut down Outcome - interruption.
	Networking components, when they are in need of substitution, may wait for a long time to be done. NCs are very costly and thus it is required to have time to prepare a sufficient budget.	Asset – PCs Actor – Unavailability of Network components for substitution Outcome - interruption.
Other problem	Network must be kept running 24/7. Thus, if the power system supply is unstable or shut down, the Network will be seriously affected in terms of loss/destruction of network administration information or performance interruption.	Asset – NCs Actor – Power supply problem Outcome - loss/destruction, interruption.
	Fire or thunder could occur at any time and their consequences are incalculable. NCs will be heavily damaged and understandably, network performance will be interrupted.	Asset – NCs Actor –Flood/Explosion/Magnetic force /Fire/Thunder Outcome - loss/destruction, interruption.

	Although keeping and maintaining PCs as well as NCs are the main tasks of the technical team, discontinuity of the team support could take place at any time due to a large amount of work, which they have to solve simultaneously. Network may occasionally encounter operational performance.	Asset – NCs Actor – Unavailability of technical team support Outcome - interruption.

Technical team		
Threat type	*Areas of concern*	*Threat Properties*
Other problems	To perform safely and stably, ECC's computing facilities require much of up-to-date expertise and skills to deal with information security. So far, the technical team has attended no professional training on this issue. Lack of such training on advanced security technology and management could result in inefficiency in running the entire computing facilities, especially in today's complicated context. When incidents happened, it would hard for technical team to respond timely and effectively. Loss/destruction or interruption of information system is inevitable.	Asset – Technical team Actor – Lack of training on security technology and management Outcome – interruption, loss/destruction
	In order to run effectively, the team must be provided with sufficient fund to cover lots of expenses such as purchasing scanning and testing software tools (i.e. virus scanning, vulnerabilities scanning tools); advanced security protection technological devices (i.e. intrusion detection system – IDS, intrusion prevention system – IPS, etc.); upgrading existing physical infrastructure (i.e. locks, doors or windows) and so forth. Once the above-mentioned things are not included in the security plan, ECC can suffer any consequences.	Asset – Technical team Actor – Insufficient budget to ensure the team's effectiveness Outcome – loss/destruction, interruption.

	Currently, there are no clear statements of commitment and common objectives for the technical team. Team is just aware of the common objectives and performance goals of the center, which are somewhat different from that of the team. Team requires more specific objectives and commitment, roles and responsibilities in case of emergency. Otherwise, they cannot serve the center well, causing interruption to the center's performance.	Asset – Technical team Actor – Lack of clear statement of commitment, common objectives and performance goals Outcome - interruption.

APPENDIX A-7

Infrastructure Components Worksheet				
Class of Components	*Selected Component/ IP address/ Host Names*	*Rationale*	*Approach (Software scanning tools)*	*Vulnerabilities summary*
Servers	198.41.0.4 198.17.208.67 198.41.3.38			
Networking components	198.41.0.4 198.17.208.67 198.41.3.38 202.153.114.101			
PCs	200.186.94.1 206.196.128.1 203.181.106.5			

APPENDIX A-8

Note: *In the tables below:*

(***) – *High impact on the organization*

(**) – *Medium impact on the organization*

(*) – *Low impact on the organization*

Technical team			
Impact on the Organization			
Outcome	*Consider*	*Impact Description*	*Values*
Interruption	How could the *ECC's operation* be affected if the technical team (in terms of technical support) were interrupted?	- In order to operate safely and stably, the center needs full support from the technical team. Otherwise, it cannot operate at its highest capacity. - Users' and staff's performance strictly rely on computing facilities. Without help of the technical team, any incident occurring on those facilities would considerably lower their effectiveness. - Lack of timely and full support of the technical team may occasionally cause some serious damages of information assets. This is usually costly to redeem.	xxx
	How could the *user's performance* be affected if the technical team (in terms of technical support) were interrupted?		
	How could the *staff's performance* be affected if the technical team (in terms of technical support) were interrupted?		
	How could the ECC be affected *financially* if the technical team were interrupted?		

Users' data			
Impacts on the Organization			
Outcome	*Consider*	*Impact Description*	*Values*
Disclosure	How could *the individual (user) property/ effort* be affected if the users' data were disclosed? How could *the user confidence* be affected if the users' data were disclosed?	The consequences are as followed: - Some people could take the disclosed data and use as their own property/work (data). This is especially dangerous when users did spend much time and efforts to create. - Users' confidence could be undermined. They would not store their important data at the center anymore, insisting on the fact that keeping the data in such an easily stolen place is very risky.	xx
Modification	How could *the user performance* be affected if the users' data were modified? How could *the individual (user) property/effort* be affected if the users' data were modified? How could *the user confidence* be affected if the users' data were modified?	Users' data requires efforts and time to be created. Thus, if they were changed, users would feel much stressed due to the thought that they would either re-create their important data (re-doing the data is by no means easy) or never get them back again. User confidence may gradually lost. They may seek another place to work on the data.	xxx
Destruction/ Loss	How could *the user performance* be affected if the users' data were destroyed? How could *the individual (user) property/ effort* be affected if the users' data were destroyed? How could *the user confidence* be affected if the users' data were destroyed?	The consequences are as followed: - Users could not perform their works for several days due to data loss/destruction. - All of efforts and time disappear in a moment. - Valuable and important works may not be recovered. It may be too late. - This loss/destruction really strike the users' spirit. It takes ages to fresh their mind again.	xxx

Interruption	How could *the user performance* be affected if the users' data were interrupted?	Users, once they are inaccessible to their data, would experience difficulties such as: - time limitation (i.e. deadline), - work continuity	xx
	How could *the individual (user) property/ effort* be affected if the users' data were interrupted?		

Management data			
Impacts on the Organization			
Outcome	*Consider*	*Impact Description*	*Values*
Disclosure	How could *the ECC's operation* be affected if the management data were disclosed? What *rules/regulations/legal penalties* could be imposed as a result of disclosure of management data? How could the ECC be affected *financially* if management data were disclosed?	- Hackers or thieves will know what ECC possesses and thus, they find it easier to do their unauthorized intentions. Financial loss and negative influence in operation are inevitable. - External organizations and people will use the financial/accounting figures, personal information and especially contract information with third-parties for their negative purposes. This goes against the benefits of the Faculty.	xxx
Modification	How could *the ECC's operation* be affected if the management data were modified? How is *the influence on other systems* as a result of modification of management data? How could the ECC be affected *financially* if management data were modified?	- The operation is heavily dependent on management data. Once they were modified, the center's operation level could be decreased. - Other systems (i.e. UIPS) are partially dependent on management data. As a result of this modification, other systems either cannot work normally or produce wrong output. - Once financial/accounting data were modified, the center would probably suffer a financial loss.	xx

Loss/ destruction	How could *the ECC's operation* be affected if the management data were destroyed?	- The operation is heavily dependent on management data. Once they were lost/destroyed, the center's operation level may be remarkably decreased. - Other systems (i.e. UIPS) are partially dependent on management data. Once they were lost/destroyed, other systems either cannot work normally or produce wrong output. - Once financial/accounting data were lost/destroyed, the center would probably suffer a financial loss.	xxx
	How is *the influence on other systems* as a result of loss/destruction of management data?		
	How could the ECC be affected *financially* if management data were destroyed?		
Interruption	How could *the ECC's operation* be affected if the management data were interrupted?	- The operation is heavily dependent on management data. Once they were interrupted, the center's operation level could be somewhat decreased. - Other systems (i.e. UIPS) are partially dependent on management data. Once they were interrupted, other systems either cannot work normally or produce wrong output. - Once financial/accounting data were interrupted, the center would probably suffer a financial loss.	x
	How is *the influence on other systems* as a result of interruption of management data?		
	How could the ECC be affected *financially* if management data were interrupted?		

UIPS			
Impacts on the Organization			
Outcome	*Consider*	*Impact Description*	*Values*
Disclosure	How could *the user's confidence* be affected if the UIPS were disclosed?	Email system, an indispensable part of UIPS, is a good illustration. Once such a system were disclosed, user's confidence would be seriously evaporated. Personal matters should not be exposed to any objectives for any reasons.	xx
Modification	How could *the ECC's operation* be affected if the UIPS were modified?	The UIPS is an important function of ECC. Thus, ECC's operation requires correct UIPS's configuration. A few changes (i.e. parameters, values, etc.) can make the center work abnormally. Next, users may feel inconvenient when working with an instable email system. Additionally, staff's performance cannot be efficient.	xxx
	How could *the user's confidence* be affected if the UIPS were modified?		
	How could *the staff's performance* be affected if the UIPS were modified?		
	How is *the influence on other systems* as a result of modification of UIPS?	UIPS has closely related to other systems (i.e. finance/accounting, services, etc.) of the center. Some vital changes (i.e. configuration, values, algorithm, etc.) can make the entire system run abnormally. Moreover, such modification can also exert a negative financial influence on the center.	xxx
	How could the ECC be affected *financially* if the UIPS were modified?		

Destruction/ Loss	How could *the ECC's operation* be affected if the UIPS were destroyed?	To work efficiently, ECC's operation requires completeness of UIPS's configuration. A few losses (i.e. inputs, parameters, values, etc.) can make the center work abnormally. What's more, users may feel inconvenient when working with a damaged email system. Besides, staff's performance could be slow down.	xxx
	How could *the staff's performance* be affected if the UIPS were destroyed?		
	How could *the user's confidence* be affected if the UIPS were destroyed?		
	How is *the influence on other systems* as a result of destruction/loss of UIPS?	- Other systems (i.e. finance/accounting, services) are partially dependent on UIPS. Once they were lost/destroyed, other systems either work abnormally or produce wrong output. - Once the UIPS's configuration and its associated data were lost/destroyed, the center would probably suffer a financial loss.	xx
	How could the ECC be affected *financially* if the UIPS were interrupted?		
Interruption	How could *the ECC's operation* be affected if the UIPS were interrupted?	The stability of the center needs UiPS continuity. Thus, an interruption may somewhat decrease the center's operation level.	xx
	How could *the staff's performance* be affected if the UIPS were interrupted?	- UIPS has links to other systems (i.e. finance/accounting, services, etc.) of the center. An interruption of UIPS also means instability in other systems/components. - Administration staff rely on the system for processing users' information. Their tasks may be halted.	xx
	How is *the influence on other systems/components* as a result of interruption of UIPS?		
	How could the ECC be affected *financially* if the UIPS were interrupted?		xx

PCs			
Impacts on the Organization			
Outcome	*Consider*	*Impact Description*	*Values*
Disclosure	How could *the user's confidence* be affected if the information on the PC screen were disclosed?	Users may feel unsafe to work on PCs, insisting on the fact that someone may either view or use what they do.	x
	How could *the individual (user) property/ effort* be affected if the information on the PC screen were viewed (disclosed)?	Information from the PCs, a long-term effort/work of users, may be viewed and taken by other people. In some cases, they must re-do their works or lose them forever.	xx
Modification	How could *the user's performance* be affected if the PCs were modified?	- Users find it inconvenient and time-consuming when working on PCs. - Staff feel inconvenient when working on PCs. Their effectiveness at work might be slightly decreased. - PCs control the operation of some components/devices (i.e. camera, printers, scanners, etc.). Modification of PC's physical or logical configuration may result in instability of those components/devices.	x
	How could *the individual (user) property/effort* be affected if the PCs were modified?		
	How could *the staff's performance* be affected if the PCs were modified?		
	How is the *influence on other systems/components/device* as a result of modification of PCs (in terms of logical or physical configuration)?		
	How could the ECC be affected *financially* if the PCs were modified (in terms of logical or physical configuration)?	PCs are one of the most valuable assets of the center. Therefore, any changes especially in physical configuration may result in a financial damage.	xx

Destruction/ Loss	How could *the user's performance* be affected if the PCs were destroyed?	- Users find it inconvenient and time-consuming when working on PCs. - Staff feel inconvenient when working on PCs. Their effectiveness at work might be slightly decreased.	x
	How could *the individual (user) property/ effort* be affected if the PCs were destroyed?		
	How could *the staff's performance* be affected if the PCs were destroyed?		
	How could the ECC be affected *financially* if the PCs were destroyed (in terms of logical or physical configuration)?	PCs are one of the most valuable assets of the center. Therefore, any damage especially in physical configuration can result in a financial loss.	xx
	How is the *influence on other systems/components/device* as a result of loss/destruction of PCs (in terms of logical or physical configuration)?	PCs control the operation of some components/devices (i.e. camera, printers, scanners, etc.). Loss/destruction of PC's physical or logical configuration may result in instability of those components/devices.	x
Interruption	How could *the ECC's operation* be affected if access to PCs were interrupted?	PCs are important tools for main functions of ECC. An interruption of these tools means a remarkable decrease in operation level.	xx
	How could *the user's performance* be affected if access to PCs were interrupted?	PCs are the main objectives for users. An interruption of these tools means that users must either seek other computing places or self-manage. Worse yet, an interruption of utilization causes severe difficulties for those who cannot backup their work/effort in time.	xxx
	How could *the individual (user) property/effort* be affected if access to PCs were interrupted?		

	How could *the staff's performance* be affected if access to PCs were interrupted?	PCs are a means for staff to communicate and process important information. Hence, staff may encounter some problems of time, accumulation of large amount of work and efficiency. Moreover, interruption of PCs operation is the reason of instability or ineffectiveness of many systems/components/device, which are linking to PCs.	xx
	How is the *influence on other systems/components/device* as a result of inaccessibility to PCs?		

NCs			
Impacts on the Organization			
Outcome	*Consider*	*Impact Description*	*Values*
Disclosure	How could the *ECC's operation* be affected if the NCs (in terms of logical configuration and administration information) were disclosed?	- Network and networking components (NCs) form the backbone of ECC's entire communication. Disclosure of NC-related information may result in increasing attacks on or intrusions into Network and thus, severely striking ECC's operation. In some cases, ECC may need some support from the Faculty to fully recover. - Users work on PCs and store their important data in shared network drives. Disclosure means such data cannot be secure. Confidence would somehow be evaporated. - ECC's Network is an indispensable part of CHULANET. A disclosure puts CHULANET in insecure manner and thus, going against the Faculty and University's rules/regulations.	xx or xxx
	How could *the user's confidence* be affected if the NCs (in terms of logical configuration and administration information) were disclosed?		
	What *rules/regulations/legal penalties* could be imposed as a result of disclosure of NCs (in terms of logical configuration and administration information)?		

Modification	How could the *ECC's operation* be affected if the NCs (in terms of logical or physical configuration and administration information) were modified?	- A modification of NCs could result in inefficiency or instability of ECC's communication activities. Consequently, the center must lower its operation level. - Working on PCs, users and staff are also members of NCs. As such, an adverse modification would remarkably affect users' and staff's performance. - NCs are one of the most valuable assets of the center. Therefore, any modification especially in physical configuration can result in a financial loss. - Any system/component/device needs a medium to communicate with the others. Understandably, a modification of this medium would considerably affect them.	xx
	How could *the user's performance* be affected if the NCs (in terms of logical configuration and administration information) were modified?		
	How could *the staff's performance* be affected if the NCs (in terms of logical configuration and administration information) were modified?		
	How could the ECC be affected *financially* if the NCs were modified (in terms of logical or physical configuration and administration information)?		
	How is the *influence on other systems/components/device* as a result of modification of NCs (in terms of logical or physical configuration and administration information)?		

Destruction/ Loss	How could the *ECC's operation* be affected if the NCs (in terms of logical or physical configuration and administration information) were lost/destroyed?	- Loss/destruction of NCs could result in instability or cease of ECC's communication activities. Consequently, the center must lower its operation level. - Working on PCs, users and staff are also members of NCs. As such, loss/destruction would heavily affect their performance. - NCs are one of the most valuable assets of the center. Therefore, any loss/destruction especially in physical configuration can result in a financial loss or even going against the Faculty's rules and regulations (e.g. in terms of asset protection) . - Any system/component/device needs a medium to communicate with the others. Understandably, a loss/destruction of this medium would seriously disrupt their performance.	xxx
	How could *the user's performance* be affected if the NCs (in terms of logical configuration and administration information) were lost/destroyed?		
	How could *the staff's performance* be affected if the NCs (in terms of logical configuration and administration information) were lost/destroyed?		
	What *rules/regulations/legal penalties* could be imposed as a result of loss/destruction of NCs (in terms of logical configuration and administration information)?		
	How could the ECC be affected *financially* if the NCs were lost/destroyed (in terms of logical or physical configuration and administration information)?		
	How is the *influence on other systems/components/device* as a result of loss/destruction of NCs (in terms of logical or physical configuration and administration information)?		

Interruption	How could the *ECC's operation* be affected if the NCs were interrupted?	- Interruption of NCs could result in a halt of ECC's communication activities. Consequently, the center must lower its operation level to the lowest. - Working on PCs, users and staff are also members of NCs. As such, an interruption would heavily disrupt their performance. - NCs are one of the most valuable assets of the center. Therefore, any loss/destruction especially in physical configuration can result in a financial loss or even going against the Faculty's rules and regulations (e.g. in terms of asset protection). - Network is a medium of communication among many systems/components/devices. Obviously, a loss/destruction of this medium would seriously strike them.	xxx
	How could *the user's performance* be affected if the NCs were interrupted?		
	How could *the staff's performance* be affected if the NCs were interrupted?		
	What *rules/regulations/legal penalties* could be imposed as a result of interruption of NCs?		
	How could the ECC be affected *financially* if the NCs were interrupted?		
	How is the *influence on other systems/components/device* as a result of interruption of NCs?		

APPENDIX A-9

Evaluation Criteria			
Impact Area	*Impact Level*		
	High	*Medium*	*Low*
ECC's operation	▪ ECC's operation sharply decreased by at least 50%. ▪ Lots of effort and expense required to recover. ▪ Need full support from other organizations in the Faculty.	▪ ECC's operation remarkably decreased by 20% to less than 50%. ▪ Some effort and expense required to recover. ▪ Might need support from other organizations in the Faculty.	▪ ECC's operation somewhat decreased by less than 20%. ▪ Little effort and expense required to recover. ▪ Be able to run independently.
User's performance	▪ Users unable to perform work for one or more days. ▪ Seriously affected; Irrecoverable loss of time/schedule.	▪ Users unable to perform work for less than a day. ▪ Remarkably affected; Efforts required to redeem time/schedule.	▪ Users unable to perform work for less than an hour. ▪ Slightly affected; Inconvenience and time-consuming.
User's confidence	▪ More than 30% drop in users due to loss of trust. ▪ Users driven either seek other places or self-manage. ▪ Center's effectiveness seriously reduced – Problems regarding Mission & Objectives	▪ From 10% to 30% drop in users due to loss of trust. ▪ Negative users' complaints. ▪ Center's effectiveness reduced - Few problems regarding Mission & Objectives	▪ Less than 10% drop in users due to loss of trust. ▪ Few negative users' complaints. ▪ Center's effectiveness slightly reduced.

Staff's performance	▪ Staff unable to perform work for one or more business days. ▪ Heavily affected; Irrecoverable loss of time/schedule ▪ Motivation affected; Effectiveness decreased	▪ Staff unable to perform work for less than a business day. ▪ Remarkably affected; Some efforts required to redeem time/schedule. ▪ Effectiveness decreased	▪ Staff unable to perform work for less than an hour. ▪ Inconvenience; Minimally affected. ▪ Effectiveness somewhat decreased
Rules/ Regulations/ Legal penalties	High-profile, in-depth investigation into organizational practices initiated by either Faculty of Engineering or the University.	Reports or records (low-profile) requested by the Faculty of Engineering and the University.	No queries from the Faculty of Engineering.
Financial	▪ More than 20,000 baht (e.g. buying new devices/components, enhancing security measures, etc.) ▪ Irredeemable errors in funding (expensive and rare devices/components, intellectual property, copyright, etc).	▪ From 1,000 baht to 20,000 baht (e.g. for repairing or replacing small damages) ▪ Partially redeemable errors in funding.	▪ Less than 1,000 baht ▪ Inconvenient; fully redeemable errors in funding.
Individual property/effort	Irrecoverable loss of individual work effort (long-term work, intellectual project/property, etc.)	Remarkably affected; Efforts required to recover the loss	Inconvenience; Minimally affected

Influences on other systems/ Components/ Devices	▪ Severely influenced; Other systems/components/devices out of order for one or more business days. ▪ May experience some irrecoverable or irredeemable losses in terms of logical or physical. configuration.	▪ Remarkably influenced; Other systems/components/devices out of order for less than a business day. ▪ Partially recoverable or redeemable; Lots of efforts spent to recover.	▪ Minorly influenced; Other systems/components/devices out of order for less than an hour. ▪ Inconvenience; Quickly recoverable

APPENDIX B

APPENDIX B-1

1. User responsibilities: Password use

The purpose of this policy is to provide users with some good security practices on using password to access data.

All users, when accessing to data, should:

(a) keep password confidential;

(b) avoid keeping a paper record of passwords, unless this can be stored securely;

(c) change passwords whenever there is any indication of possible system or password compromise;

(d) select quality passwords with a minimum length of eighth characters which are difficult to guess because they:

- have both upper case and lowercase letters
- have digits and/or punctuation characters as well as letters
- may include some control characters and/or spaces
- are easy to remember, so they do not have to be written down

(e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

(f) change temporary passwords at first log-on;

(g) not include passwords in any automated log-on process (e.g. passwords stored in a macro, function key);

(h) not share individual user password; If so, after finishing, change it;

(i) not record passwords online (e.g. in a file, in a database, in email or in SMS messages);

(j) be aware of social engineering to identify passwords (e.g. an email or telephone from someone asking passwords to check data);

(k) be aware of password sniffers (e.g. avoiding protocols that send passwords in clear text) and stealers (e.g. programs or physical devices that record the key-strokes);

2. User password management

This policy aims at preventing unauthorized access to users' data.

The center, when managing user password, should:

(a) check that the user has authorization from the system administrator for the use of information system or services. Separate approval for access rights from management is required;

(b) check that the level of access granted is appropriate to the user's purpose and is consistent with the organizational security policy;
(c) give users a written statement of their access rights;
(d) require users to sign statements indicating that they understand the conditions of access (e.g. to keep their passwords confidential);
(e) maintain a formal record of all users registered to use services. This record should be kept confidential, accurate and complete;
(f) immediately remove access rights of users who have graduated or left the Faculty of Engineering;
(g) periodically check for, and remove redundant user IDs and accounts;
(h) ensure that redundant user IDs are not issued to other users;
(i) ensure that temporary passwords are given to users in a secure manner. The use of third-parties or unprotected means (e.g. telephone asking, email) should be avoided. Users should acknowledge receipt of passwords and change temporary passwords immediately;

3. Review of user access rights

This policy is to maintain the effective control over access to data. Conducting a formal process to review user's access right every two months and after any changes is necessary.

4. Backup data

The purpose of this policy is to maintain the integrity and availability of information that is critical to the business objective and operation of the center.

The center should:

(a) provide adequate backup facilities to ensure that software, management data and important users' data, system and network's data can be recovered following an incident or breach;
(b) test backup arrangement for individual systems for every month to ensure that they meet the requirements of business continuity plans (see Clause 34);
(c) make backup copies of software, management data, important users' data, system and network's data for every four months, two weeks, one week, and two weeks, respectively;
(d) store a minimum level of backup information (i.e. 30% of the total), together with accurate and complete records of the backup copies and documented restoration

procedures, in a remote location, at a sufficient distance to escape any damage from an incident at the main site. At least three generations or cycles should be retained;

(e) give backup information an appropriate level of physical and environmental protection (see Clause 22.6) that is consistent with the standard applied at the main site;

(f) test backup information every two months to ensure that they can be relied upon for emergency use when necessary;

(g) check the restoration procedures every four months for effectiveness;

(h) determine the retention period for backup information;

(i) migrate the data on backup drives each time the center purchases a new backup system;

(j) keep the information on backup (i.e. location, contents, etc.) confidential. Such information should be delivered to head of the center and manager of technical team;

(k) ensure that staff are not allowed, or have the opportunity to alter, deface or remove any part of the users' data or management data contained in the center's data storage.

(l) establish procedures so that comments from users are reviewed;

APPENDIX B-2

5. Access control to program source library

The purpose of this policy is to reduce the potential for corruption of computer programs.

The center should maintain strict control over access to program source libraries as follows:

(a) where possible, program source libraries should not be held in operational systems;

(b) technical staff should not have unrestricted access to program source libraries;

(c) programs under development or maintenance should not be held in operational program source libraries;

(d) the updating of program source libraries and the issuing of program sources to install should only be performed by a nominated technical staff upon the authorization from the head of the center;

(e) program listing should be held in a secure environment (e.g. such documents stored online should be encrypted);

(f) an audit log should be maintained of all accesses to program source libraries;

(g) old versions of source programs should be archived, with a clear definition of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures;

6. Inventory of physical assets

This policy aims at substituting the protection of the center's physical assets (e.g. hardware, power supplies, air-conditioning units, etc).

The center needs to be able to identify its assets and the relative value and importance of these assets. Then, the center should draw up inventory commensurate with the identified value and importance of the assets. When planning inventory, the center should also take into account the business continuity plan (see Clause 34)

7. Controls against malicious software

This policy is to offer detection and prevention controls against malicious software as well as appropriate user awareness procedures.

The center should:

(a) prohibit the use of unauthorized software. Software should be from a trusted source or an official vendor with certified stamp;

(b) strictly control and minimize the use of files and software, either free or commercial, obtained from or via external networks or on any other medium;

(c) always install and update anti-virus detection and repair software to scan computers and media when necessary or on a routine basis;

(d) conduct reviews of the software and data content of systems supporting critical business processes monthly. The presence of any unapproved files or unauthorized amendments should be formally investigated;

(e) always check any files on electronic media of uncertain or unauthorized origin, files received from unknown or untrusted networks, email attachments for viruses before use. Checking should be performed at different places (e.g. on Web servers, Mail servers, desktops, routers, etc.);

(f) strictly follow the incident reporting procedures (see Clause 26) as well as the business continuity plan (see Clause 34);

(g) continually monitor the contour of malicious software in the world. Warnings from security experts as well as prestigious organizations should be treated at the highest priority. Manager of the technical team should ensure that qualified sources (e.g. reputable journals, reliable Internet sites or anti-virus software suppliers) are used to detect and work out the problems. All staff should be aware of the incident reporting procedures (see Clause 26) and technical staff should know what to do following an incident caused by malicious software;

8. Reporting security incident

The goal of this policy is to minimize the damage from security incidents and to monitor and learn from such incidents.

The center should ensure that:

(a) all staff are aware of different types of security incidents (security breach, threat, weakness or malfunction) and how to report to head of the center or manager of technical team as quickly as possible;

(b) feedback and results of how the incidents have been dealt are informed and documented;

(c) incidents can be used in training on security awareness as examples of what could happen, how to respond and how to avoid them in the future;

9. Reporting software malfunction

This policy aims at detecting software malfunctions that can have impact on the center's data and systems.

The center should ensure that:

(a) the symptoms of the problems and any messages appearing on the screen are noted;

(b) the computer is isolated, if possible, and its operation is stopped. Appropriate contacts should be alerted. If equipment is to be examined, it should be disconnected from any organizational networks before being re-started. Data and software on the examined computer should not be transferred to other computers;

(c) the matter is immediately reported to manager of technical team;

(d) users and staff do not remove the suspected software or files unless authorized to do so;

(e) only designated technical staff and experts can carry out the investigation and recovery procedures;

10. Cryptographic controls

This policy aims at enhancing the protection of sensitive or critical information of the center such as important users' data, management data or system by adopting encryption techniques.

The center should ensure that

(a) consider and apply appropriate encryption techniques (i.e. hardware and software) for each of the above mentioned information assets;

(b) users, if possible, can be provided with some simple encryption techniques to control the access to their sensitive or critical data;

(c) encryption system adopted for management data or other systems should be up-to-date and effective. Only authorized staff can access to these assets. Staff should strictly follow policy on the use of cryptographic controls (see Clause 16);

11. Support for purchased information assets

This policy is to enhance the quality of the purchased software and hardware, thereby minimizing the potential of suffering defects.

The center should

(a) ensure that the vendors who supply hardware and software products should qualify for international standards (e.g. ISO 9001, ISO 14001, etc.). All products should bear the certified true stamp of the manufacturer and the warranty;

(b) all software and hardware products, before purchasing, should be thoroughly tested and qualified for standards set up and guaranteed by prestigious organizations in Thailand. Any suspicion of the operational quality should be fully investigated and solved out immediately. Checking results should be documented.

(c) keep in touch with the vendors for continual technical support. In case of urgent support, a minimum time of 2 hours are required for the vendors to be in site;

(d) donated software and hardware products should also go through thorough quality testing before use. Only those qualified for standards set up by prestigious organizations in Thailand are ready for use. In case of absent vendor support, due care for maintenance and operation should be taken;

APPENDIX B-3

12. Power supplies

This policy is to ensure the operational continuity of information assets (e.g. accessing and using users' data and management data, running system, PCs and NCs) at the center in terms of avoiding power failures and electrical anomalies.

The center may choose the following options:

(a) multiple feeds to avoid a single point of failure in the power supply;

(b) uninterruptable power supply (UPS);

(c) back-up generator;

At least, the center should ensure that

(d) some PCs are selected to be equipped with the above-mentioned options so that they fully serve admin staff to access management data and some users who are in need of accessing and using their data continuously;

(e) time to re-access management data and important users' data, in case of power failure, should not exceed one business-hour;

(f) power system feeding for some important systems (e.g. UIPS), network and networking components are available 24/7;

(g) testing on the quality and status of those electric-feeding or generating equipment are carried out every month. Preparation for power failures and electrical anomalies should be in accordance with the business contingency plan (See Clause 34);

(h) backup electric-feeding or generating equipment are also prepared;

(i) safety of power system is also taken into account. During running physical assets, there is no electric shock or incident.

APPENDIX B-4

13. Policy for accessing to business information and application system

This policy aims at controlling access to business information or application system.

It's necessary to address the two issues:

(a) management data include users' 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. Thus, security requirement for management data is confidentiality.

(b) UIPS is a system that manages user-related data (i.e. printing, accounts, FTP services, storage, etc.) including email system at the center. Thus, security requirement for UIPS is integrity;

Working with management data and UIPS requires staff to strictly follow principles below:

(c) management data and UIPS should be kept confidential, accurate and complete. Only authorized or designated staff are able to access to them. Any other people attempting to access the data or system are considered illegal. In that case, such access should be informed to head of the center and manager of technical team immediately and there should be a check for the data's or system integrity and confidentiality (in terms of the disclosure or viewing level);

(d) staff (1) who directly or indirectly discloses/modifies/destroys/interrupts UIPS or management data without authorization or (2) who directly or indirectly enables unauthorized people to access data or system is considered a violator of information security, who will be subject to the Disciplinary process (see Clause 32);

(e) access to management data or UIPS should be monitored and recorded;

(f) management of access rights in a networked environment should be able to recognize all types of connection available (including wireless connection);

(g) access rights should be reviewed every four months;

14. Quality of processing management data

This policy is to ensure the integrity of the management data, which is important to the operational stability of the center.

Care should be taken as followed:

(a) Management data should be accurate and complete. Every reasonable step should be taken to rectify data that is inaccurate or incomplete;

Note: Corrections to management data should never delete or overwrite the original entry and/or audit trail for the original entry. The correction should append the revised data to the original entry, together with information identifying the individual who makes the correction, the date and time of the correction.

(b) The center is responsible for maintaining the completeness and accuracy of management data supported by the organizational security policies;

Note: Computer systems, which process and store management data, should be subject to periodic independent reviews (e.g. every four to six months) to ensure that the accuracy and completeness of the processed and stored data.

APPENDIX B-5

15. Review and audits of computing system

This policy is to prevent hardware failure of computing system, which may have impact on accessing to users' data or management data.

Computer systems, which process and store data, should be subject to a periodic independent inspection (e.g. every four to six months) and audit of security safeguards. In addition to those regularly scheduled, reviews should be undertaken in the following circumstances:

(a) physical move,

(b) change in hardware, software, or communications networks,

(c) change in operation, or

(d) a major security incident.

16. Policy on the use of cryptographic controls

This policy is to provide the staff with guidelines of the use of cryptographic controls, thereby enhancing protection for business information.

The following issues should be taken into account:

(a) Cryptographic controls are effective measures for protecting confidentiality and integrity. Thus, those who are assigned to keep the *'secret key'* or *'private key'* (e.g. to decrypt the encrypted information of the center) should be trusted and strictly careful. Revealing the key to unauthorized people is considered as a serious breach of information security;

(b) All keys including *'public keys'* and *'private or secret keys'* should be protected against disclosure, modification and destruction. Any behaviors attempting to do so should be considered as unauthorized accessing to the center's information assets;

(c) Physical protection should be used to protect equipment used to generate, store and archive keys;

(d) There should be contingency solution in case of losing or compromising the keys;

(e) Keys should have pre-defined activation and deactivation dates to reduce the likelihood of compromise;

APPENDIX B-6

17. Information access restriction

The purpose of this policy is to prevent unauthorized access to information held in information systems.

In each information system, the center should:

(a) provide menus to control access to application system functions;

(b) restrict staff' knowledge of information or application system functions which they are not authorized to access, with appropriate editing of staff instruction documentation;

(c) control the access rights of staff (e.g. read, write, delete, execute, etc);

(d) ensure that outputs from application system handling sensitive information contain only the information that are relevant to the use of the output and that they (the outputs) are sent only to authorized people or terminals;

18. Monitoring system access and use

This policy is to detect unauthorized access to and use of system.

Monitoring the access to and use of the information system should include:

(a) authorized access (e.g. user ID, data and time of key events, the file accessed, etc.);

(b) unauthorized access attempts (e.g. failed attempts, access policy violations and notifications for network gateways and firewalls, etc.);

(c) alerts from proprietary Intrusion Detection Systems (IDS) or Intrustion Prevention System (IPS);

(d) system alerts or failures (e.g. system log exceptions, network management alarms, etc.);

APPENDIX B-7

19. Policy on the use of email

The purpose of this policy is to prevent risks created by using emails.

Staff and users, when using emails, should be aware of:

(a) attacks or harassment on email (e.g. viruses, interception, Spam mail or Junk mail, etc.);

(b) protection of email attachment;

(c) unknown senders or unidentified attachments. In those cases, deleting all messages as well as attachments is necessary;

(d) not compromising the center (e.g. sending defamatory emails, use for harassment, etc.);

(e) the use of cryptographic techniques (see Clause 10 and 16) to protect the confidentiality and integrity of the content (e.g. using Pretty Good Privacy – PGP technique to encrypt messages, etc.);

(f) retention of messages which, if stored, could be discovered in case of litigation;

APPENDIX B-8

20. Segregation of duties

This policy is to reduce the risk of accidental or deliberate system misuse.

The center should separate the management of network from that of computing system. This would help to reduce the unauthorized modification or misuse of information system and networks.

21. Network controls

The purpose of this policy is to ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

The center should implement the following controls:

(a) Operational responsibilities for networks should be separated from computer operations where appropriate (see Clause 20);

(b) Sensitive system and network's data is protected by secure storage (e.g. backups stored off-site, discard process for sensitive information) (see Clause 4 and 22.6);

(c) All systems are up-to-date with respect to revisions, patches and recommendations in security advisories;

(d) There is a documented and tested data backup plan for backups of both network's software and data. All staff understand their responsibilities under the backup plans;

(e) Only necessary services are running on systems. All unnecessary services have been removed;

(f) Tools and mechanisms for secure system and network administration are used and they are routinely reviewed and updated or replaced;

(g) Firewall and other security components are periodically audited (e.g. for every one to two months) for compliance with policy;

(h) Appropriate access controls and user authentication (e.g. file permissions, network configuration) consistent with organizational security policy are used to restrict user access to critical business information (e.g. management data), sensitive systems (e.g. UIPS), specific applications and services over the network;

(i) The center has up-to-date diagrams that show its security architecture and network topology. Any irrelevance or change should be quickly identified and corrected for technical reference. Such information should be kept confidential, accurate and complete by authorized and trusted technical staff;

APPENDIX B-9

22. Physical security controls

This policy is to prevent unauthorized access, damage and interference to physical information assets (e.g. PCs, NCs, data storage, etc.) of the center.

22.1 Location and construction:

The following controls should be applied:

(a) Physical information assets of the center should be centrally located within a clearly defined space so as to minimize exposure to:
- fire, water, corrosive agents and smoke from adjacent areas;
- flooding;
- explosion or shock;
- unauthorized access;
- potential hazards from physically adjacent areas.

Example: Physical information assets shouldn't be built over, under or adjacent to kitchen or toilet facilities.

(b) Buildings housing the center physical information assets should conform to relevant statutory codes and standards set up by Thai government (e.g. fire, building and electrical);

(c) Entrances to areas containing Networking Components (e.g. Web and Mail servers, routers, switches, etc.) should be protected with secure doors, locking hardware and authentication devices;

Example: The room containing servers should be carefully locked and equipped with authentication devices (e.g. checking fingerprint).

(d) Water and sewage pipes should be routed far off the physical information assets storage areas. Where this is not possible, readily-accessible water shut-off valves should be provided.

22.2 Access Control and Authorization

(a) Areas where the center's data are processed and/or stored, and areas housing important Networking Components supporting the Network should be designated as secure areas.

(b) Access rights to theses secure areas should be authorized and controlled. Signs indicating "authorized personnel only" or a similar message should be prominently posted at all entrances to secure areas. Authorized staff working in these areas

should report to manager of technical team about incidents identified (see Clause 8). Management review of accessing to these areas should be carried out weekly;

(c) Unauthorized personnel and visitors who require access to secure areas should be escorted by authorized staff at all times;

(d) Provisions should be made for prohibiting unauthorized access to secure areas when the area is unattended and unoccupied.

(e) Surveillance methods (e.g. motion detectors and alarms, cameras) should be installed in all secure areas;

(f) Records, in the form of an access control log, should be kept of access to secure areas for:
- visitors;
- external maintenance and support personnel; and
- authorized personnel outside of normal business hours or assigned hours of work.

(g) The access control log should record the following information:
- identification of the person entering;
- employer or affiliation;
- identification of the individual authorizing entry;
- restricted area to be entered;
- date and time of entry; and

22.3 Fire Protection

(a) Fire protection for the center's physical information assets and data storage areas should conform with all fire regulations governing the location;

(b) Flammable materials should not be stored in areas housing the center's physical information assets and data storage;

(c) The use of materials known to produce static electricity or magnetic forces should be strictly prohibited in the center's physical information assets and data storage areas;

(d) Important physical information assets such as Networking Components (i.e. Web and Mail servers, routers, bridges, switches, etc.), PCs, data storage should be equipped with reliable devices protecting against thunderstruck. Due care should be paid to those assets when operating under thunderstruck;

22.4 Cabling security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage:

(a) Network cabling should be protected from unauthorized interception or damage (e.g. by using conduit or by avoiding routes through public areas);
(b) For sensitive or critical system, further controls should include:
   - Installation of armoured conduit and locked boxes at termination points (e.g. the hubs for connecting from PCs to network in each computer room should be put in a locked box);
   - Use of alternative routings or transmission of media;

22.5 Waste disposal

(a) The center's storage devices, records (e.g. drives, tapes, etc.), orders and other documents and recording media containing sensitive data or security control records should be destroyed in an appropriate manner (e.g. burning, shredding, disintegration);
(b) Media containing the above-mentioned data or records awaiting destruction should be stored in a secure manner;

22.6 Off-site Facilities

(a) Physical and environmental security provisions for off-site storage should conform to the same standards as primary facilities:
(b) Plans for backup facilities should ensure that physical and environmental security at the backup site can be made commensurate with the primary site;
(c) The location for off-site storage should not be subject to the same exposure to a specific threat as the primary site;

22.7 Evacuation Procedures

(a) Evacuation procedures for all areas containing the center's physical information assets and data storage should be developed, documented and disseminated. All staff should be aware of these procedures;
(b) Procedures should ensure that appropriate security is maintained during and following the evacuation;

23. Reporting security weaknesses

This policy is to minimize damage from security incidents and malfunctions and to monitor and learn from such incidents.

Staff, when using physical information assets (e.g. PCs, NCs, data storage, etc.) should be required to note and report any observed or suspected security weaknesses in, or threats to,

those physical information assets. They should report to either manager of the technical team or head of the center as quickly as possible. Users should not attempt to prove a suspected weakness since this behavior may be considered a security breach.

APPENDIX B-10

24. Documented operating procedures

This policy is to ensure the correct and secure operation of physical information assets (e.g. PCs, NCs, data storage, etc.), thereat reducing the likelihood of encountering operating/network administration software defects and hardware defects.

The operating procedures should be clearly described for each physical information asset in accordance with the organizational security policy. Procedures should specify the detailed instructions including:

(a) Processing and handling of information;
(b) Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restriction on the use of system utilities;
(c) Support contacts in the event of unexpected operational or technical difficulties;
(d) System restart and recovery procedures for use in the event of system failure;

25. Operational change control

This policy is to reduce the likelihood of encountering operating/network administration software defects and hardware defects by adequate controlling changes to physical information assets (PCs, NCs, data storage, etc.) at the center.

The following controls should be applied:
(a) Identification and recording of significant changes;
(b) Assessment of the potential impact of such changes;
(c) Formal approval procedure for proposed changes;
(d) Communication of change details to all relevant staff;
(e) Procedures identifying responsibilities for aborting and recovering from unsuccessful changes;

26. Incident response management procedures

This policy is to ensure a quick, effective and orderly response to security incidents.

The following controls should be applied:

(a) Procedures should be established to cover all potential types of security incidents, including:
- information system failures and loss/damage of information assets;
- denial of service;
- errors resulting from incomplete or inaccurate management data;
- breaches of confidentiality;

(b) In addition to normal contingency plans (see Clause 33), the procedures should also cover:
- Analysis and identification of the cause of the incident;
- Planning and implementation of the remedies to prevent recurrences, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those affected by or involved with recovery from the incident;
- Reporting the action to the manager of technical team;

(c) Audit trails and similar evidence should be collected and secured, as appropriate, for:
- Problem analysis within the technical team and with head of the center;
- Negotiating for compensation from software and hardware supplies;

27. Physical information asset maintenance

The purpose of this policy is to ensure that all physical information assets (e.g. PCs, NCs, data storage, etc.) are available and in good condition.

The following controls should be applied:

(a) Physical information assets should be maintained in accordance with the supplier's or vendor's recommendation and specification;

(b) Only authorized staff or external people should carry out repairs and service. External people from vendor or supplier, when performing maintenance, should be strictly supervised by experienced technical staff. Any suspected behavior should be immediately reported to manager of the technical team;

(c) Records should be kept of all suspected or actual faults and all preventive and corrective maintenance;

(d) Appropriate controls should be taken when sending physical information assets off premises for maintenance;

APPENDIX B-11

28. Information security management training for staff

This policy is 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.

The following issues should be applied:

(a) Management of the center should provide orientation and training on information security management to all staff and volunteers concerning the center's organizational security policies and procedures to ensure the confidentiality, integrity and availability of the center's information assets. Orientation and training programs should include:
   - awareness of organizational security policy,
   - information security trends, procedures and up-to-date best practices;
   - staff responsibilities and detailed action plan;
   - detecting and reporting information security breaches and incidents;
   - incident response program;

(b) A certificate of attendance at a security awareness or training program should be placed on the employee's personnel file.

(c) Security awareness and training programs should be provided to employees, professional staff, contract staff and volunteers on a periodic basis (e.g. annually, bi-annually) to maintain awareness and provide information about new policies or procedures.

29. Policy on the technical team's commitment and common objectives

The purpose of this policy is to guide the technical team on establishing commitment and common objectives.

The technical team's commitment and common objectives should cover the following issues:

- Maintaining information assets so that they can operate in good condition;
- Routine checking the configuration and status of information assets;
- Protecting information assets from security breaches and incidents;
- Detecting and reporting security breaches and incidents to manager of the technical team and head of the center;
- Receiving feedback from users on the operating condition as well as technical faults (in terms of hardware and software).
- Finding solution for feedback from users;
- Cooperating with management in reviewing security issues;

- Joining for incident response program;
- Ensuring the success of business continuity program following incidents;

APPENDIX B-12

30. Management information security forum

This policy is to enhance the effectiveness of information security management within the center.

Management should establish a forum that undertakes the following issues:

(a) Reviewing and approving information security policy and overall responsibilities;

(b) Monitoring significant changes in the exposure of information assets to major threats;

(c) Reviewing and monitoring information security incidents;

(d) Approving major activities to enhance information security;

31. Personnel security

This policy is to reduce the risks of human error, theft, fraud or misuse of information assets.

The following controls should be applied:

(a) Security roles and responsibilities, as laid down in the organizational security policy, should be documented and incorporated into staff's assigned tasks. It should include general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular asset, or for the execution of particular security processes;

(b) As far as the personnel's using information assets is concerned, a record should be maintained and be readily available documenting:
   - the issue and retrieval of security-related items such as keys, codes, combinations, badges and system passwords;
   - the custody and use of all information system assets (e.g. borrowing laptops, computer software, and specialized data storage);

(c) On termination or transfer of employment, or when the staff's duties no longer require access to the information assets, the center should immediately:
   - revoke access privileges (e.g. user-ID's and passwords) to system and data resources, and secure areas,

- retrieve sensitive material including access control items (e.g. keys and badges), and
- retrieve all hardware, software and documentation issued or loaned to the employee;

(d) The center should have corrective and disciplinary procedures in place to address any breach of security or privacy (see Clause 32);

(e) Staff performance reviews should be partly based on assessment on the performance related to the handling of information assets.

32. Disciplinary process

This policy is to prevent staff from compromising the center's information assets.

Management should establish a formal disciplinary process for staff who have violated organizational security policies. Such a process can act as a deterrent to staff might otherwise be inclined to disregard security procedures. Besides, it should ensure correct, fair treatment for those who are suspected of committing serious security breaches.

33. Contingency planning

This policy aims at strengthening the effectiveness of responding to security breaches and incidents leaving serious impact on the center's operation.

The following controls should be applied:

(a) Contingency plans should be developed, documented and maintained to ensure the essential level of operation that will be provided following any loss of operating capability (e.g. from the loss or destruction of a diskette storing sensitive or confidential data to the entire destruction of the computing facility). Plans should cover on-site and off-site recovery and, as a minimum, consider:
   - recovery from any failure to the system and information resources;
   - re-establishment of the information system operation, following destruction of the computing facility, using none of the systems and information resources contained within the primary facility;
   - forced evacuation of the computing facility;
   - bankruptcy of critical suppliers or vendors; and
   - loss of critical support systems.

(b) Where plans require the use of facilities not under the control of the center, formal agreements or contracts for the use of such facilities should be entered into and should be reviewed annually;

(c) Plans should include the identification of essential systems, information resources, and personnel;

(d) Planned responses to contingencies should not compromise confidentiality or integrity or availability requirements;

(e) Copies of all contingency plans, procedures and agreements should be maintained in at least two geographically separate locations. They should be kept accurate and complete;

(f) Contingency plans should be tested annually to the extent practical;

(g) There should be sufficient backup of personnel to assure the confidentiality, integrity and availability of critical systems;

(h) Personnel required to support an essential level of operation should be identified and the up-to-date list should form part of the contingency plans;

(i) Personnel identified to take an active role in contingency situations should receive training and practice in their assigned duties;

(j) Backup of the critical information and system should be prepared annually and stored at an off-site location;

(k) Current copies of the critical operational data and material and a sufficient supply of the critical media resources to ensure the continued provision of the minimum essential level of operation should be stored at an off-site location. Physical security of these items should not be different from that of other assets at the main site. These items should include:

- operating system software,
- utilities,
- applications system software,
- data,
- documentation,
  encryption keys,
- access control information (e.g. passwords), and
- forms.

(l) A contingency procedure should be developed detailing the course of action to follow when a type of security breach or incident is suspected;

34. Business continuity management plan

The goal of this policy is to counteract interruptions to operational activities and to protect critical operational processes from the effects of major failures or disasters.

A complete and efficient plan should bring together the following key elements of business continuity management:

(a) Understanding the risks the center is facing in terms of their likelihood, associated impact, and prioritization;

(b) Understanding the impact whose interruptions are likely to have on the business and establishing objectives of information assets;

(c) Considering the purchase of suitable insurance which might form part of the business continuity process;

(d) Formulating and documenting a business continuity strategy consistent with the agreed business objectives;

(e) Regular testing and updating of the plans and processes put in place (e.g. testing and updating the processes annually);

(f) Ensuring that the management of business continuity is incorporated in the center's processes and structure. Responsibilities for co-ordinating the business continuity management process should be assigned at an appropriate level within the center (e.g. at the information security forum – See Clause 30);

(g) Strict following the risk assessment to determine the impact of those interruptions to the operation of the center;

(h) Appropriate training and education of staff in the agreed procedures and processes including crisis management;

(i) Establishing the resumption procedures describing the actions to be taken to return to normal operation;

APPENDIX C

APPENDIX C-1

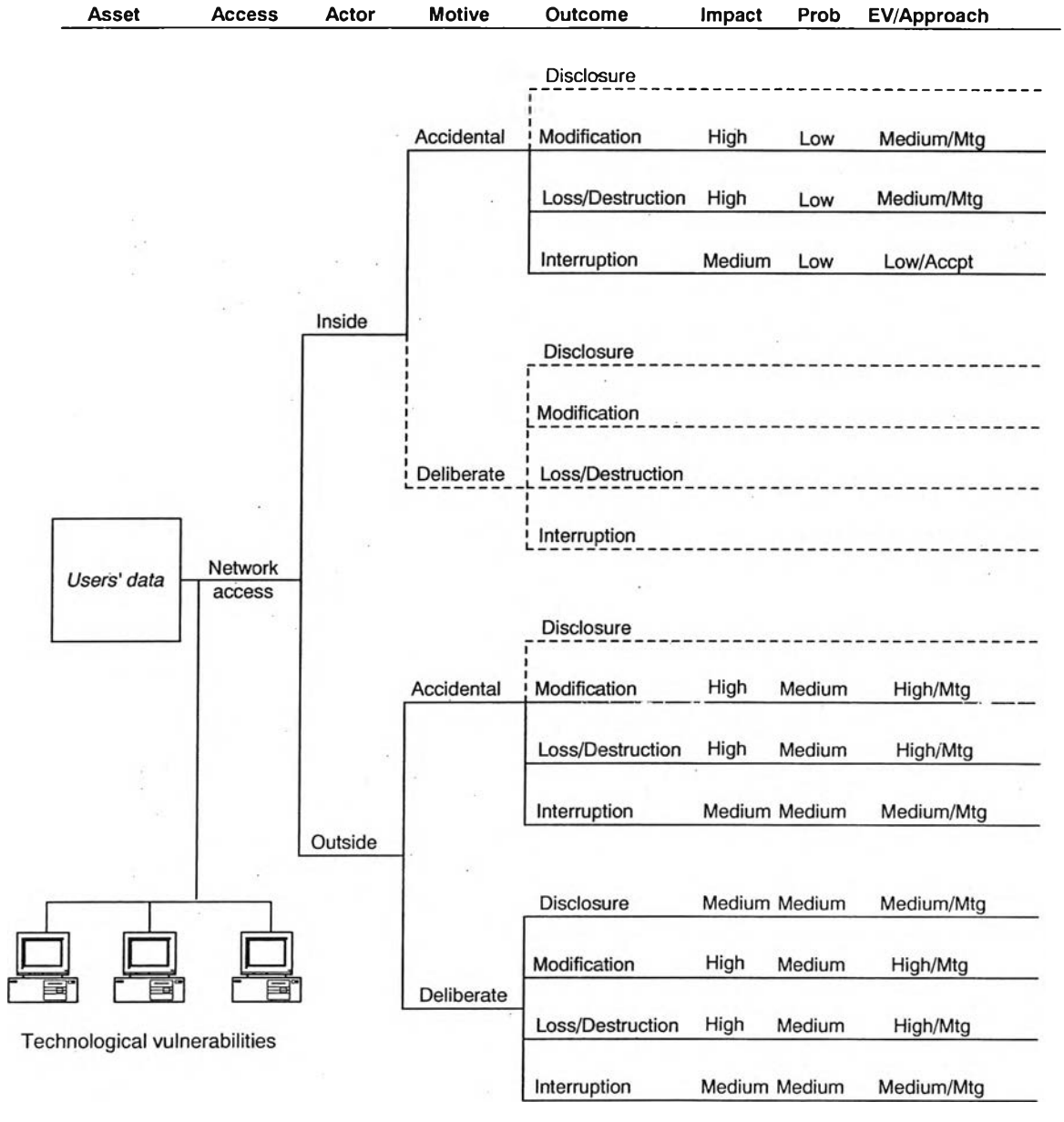

FIGURE C-1: *Users' data - Risk Profile for Human Actors Using Network Access.*

APPENDIX C-2

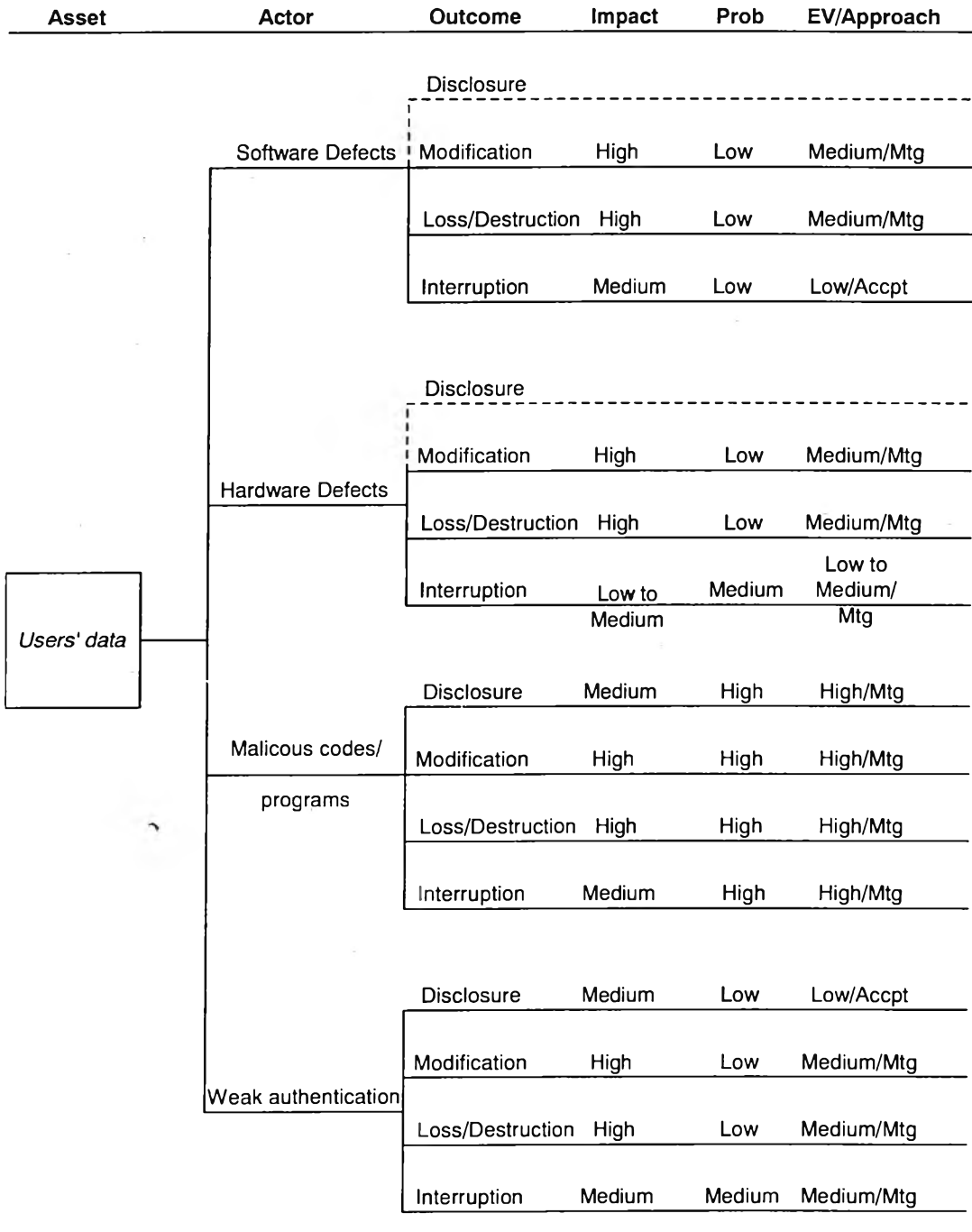

FIGURE C-2: *Users' data - Risk Profile for System Problems.*

APPENDIX C-3

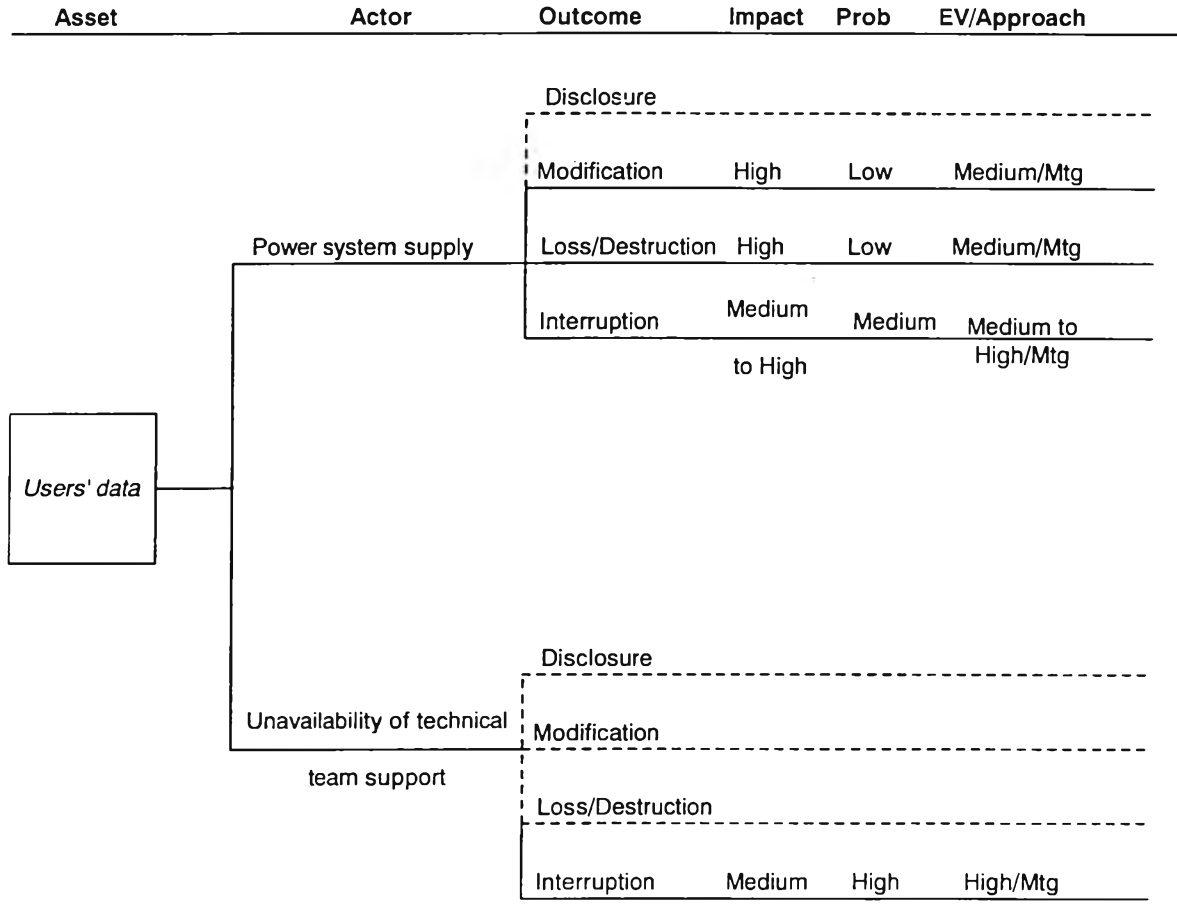

FIGURE C-3: *Users' data - Risk Profile for Other Problems.*

APPENDIX C-4

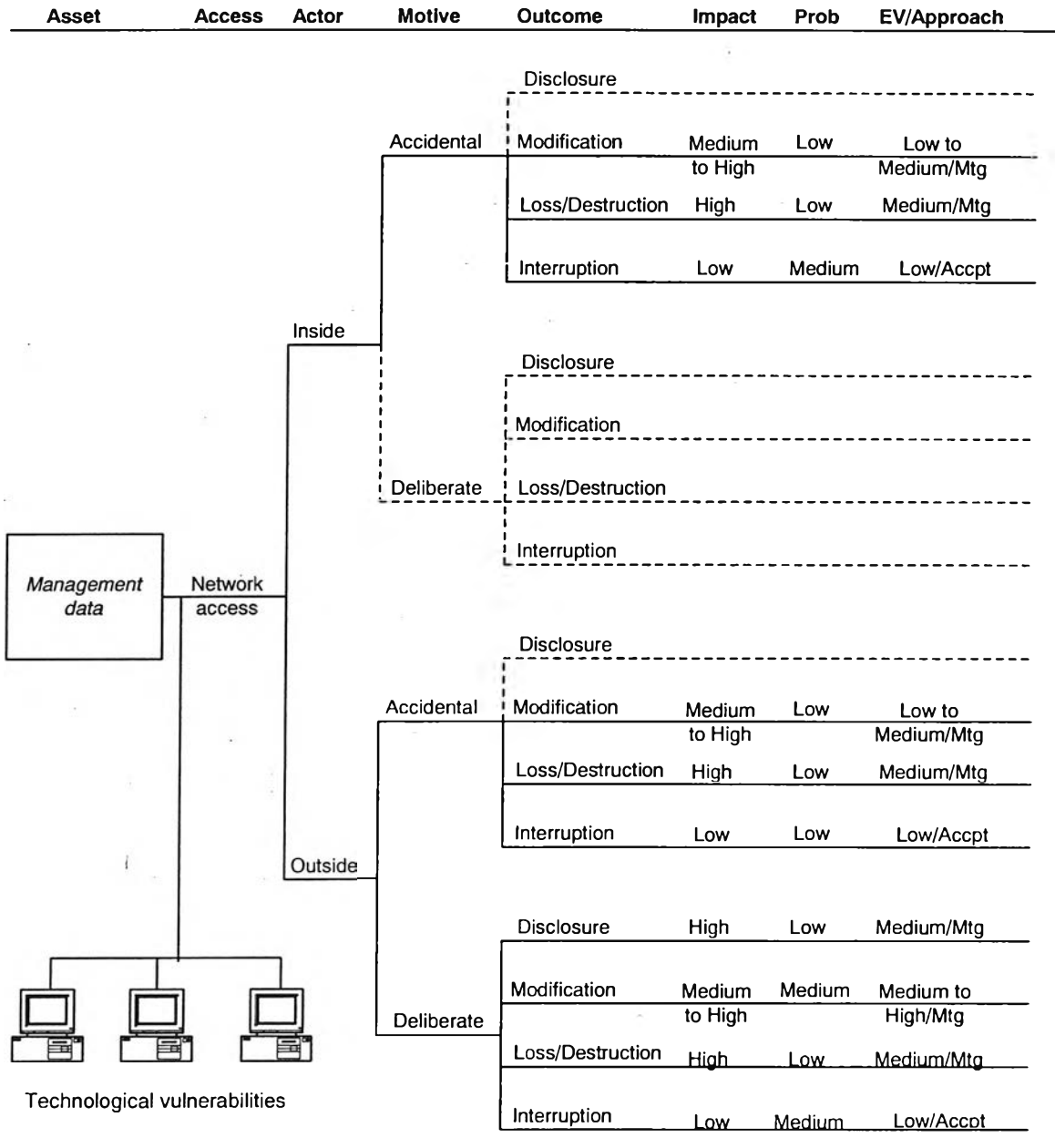

FIGURE C-4: *Management data - Risk Profile for Human Actors Using Network Access.*

APPENDIX C-5

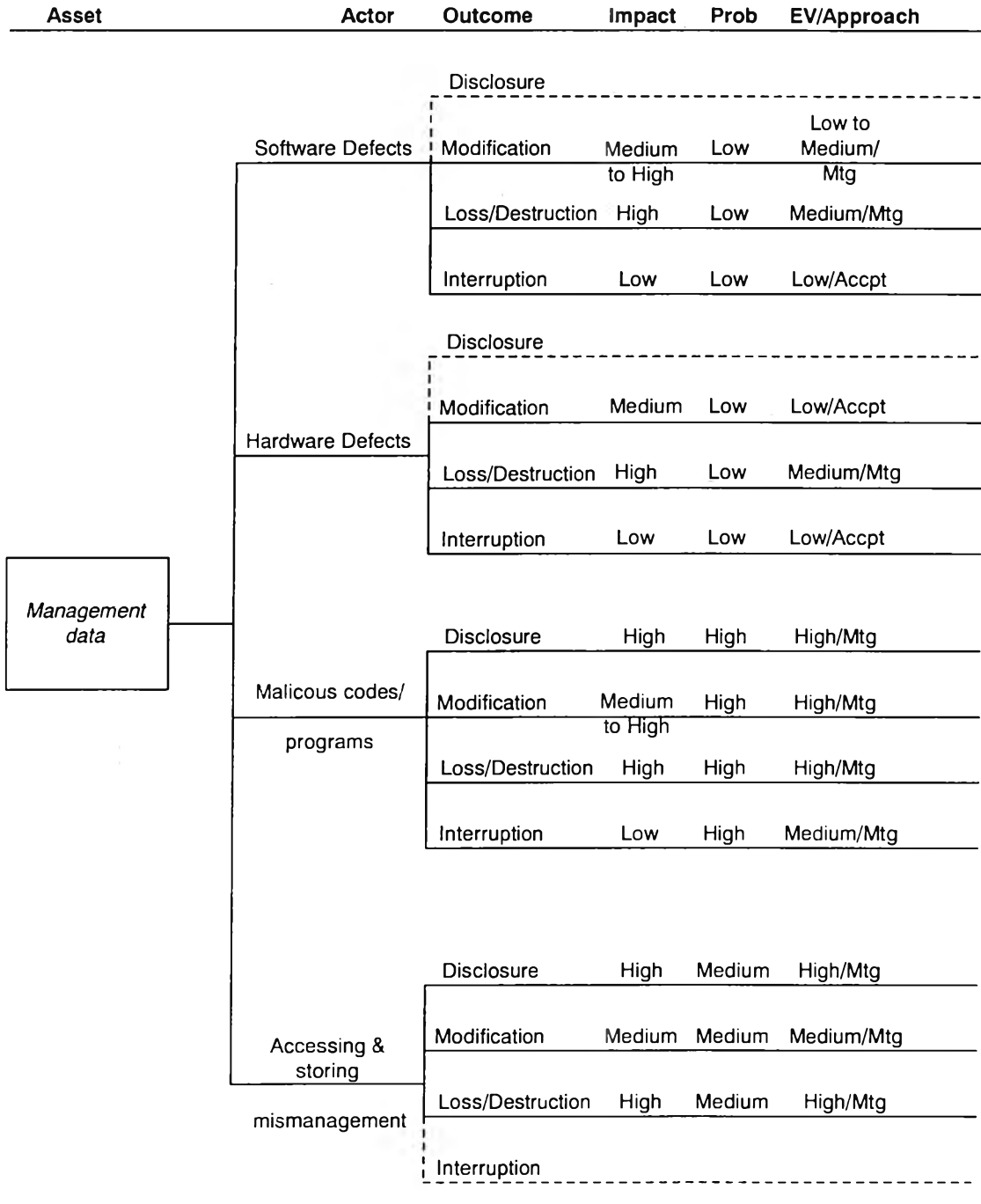

FIGURE C-5: *Management data - Risk Profile for System Problems.*

APPENDIX C-6

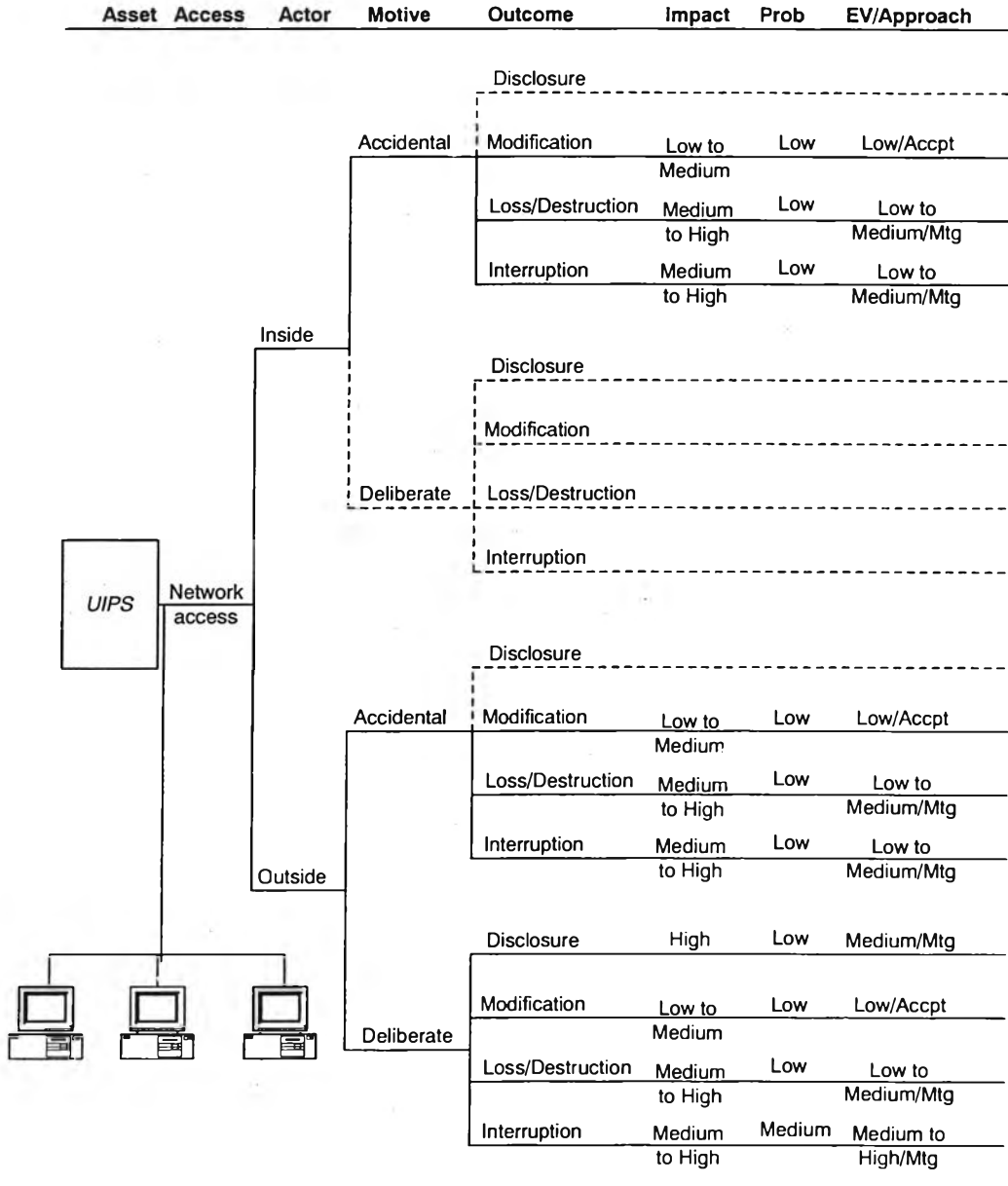

FIGURE C-6: *UIPS - Risk Profile for Human actors using network access.*

APPENDIX C-7

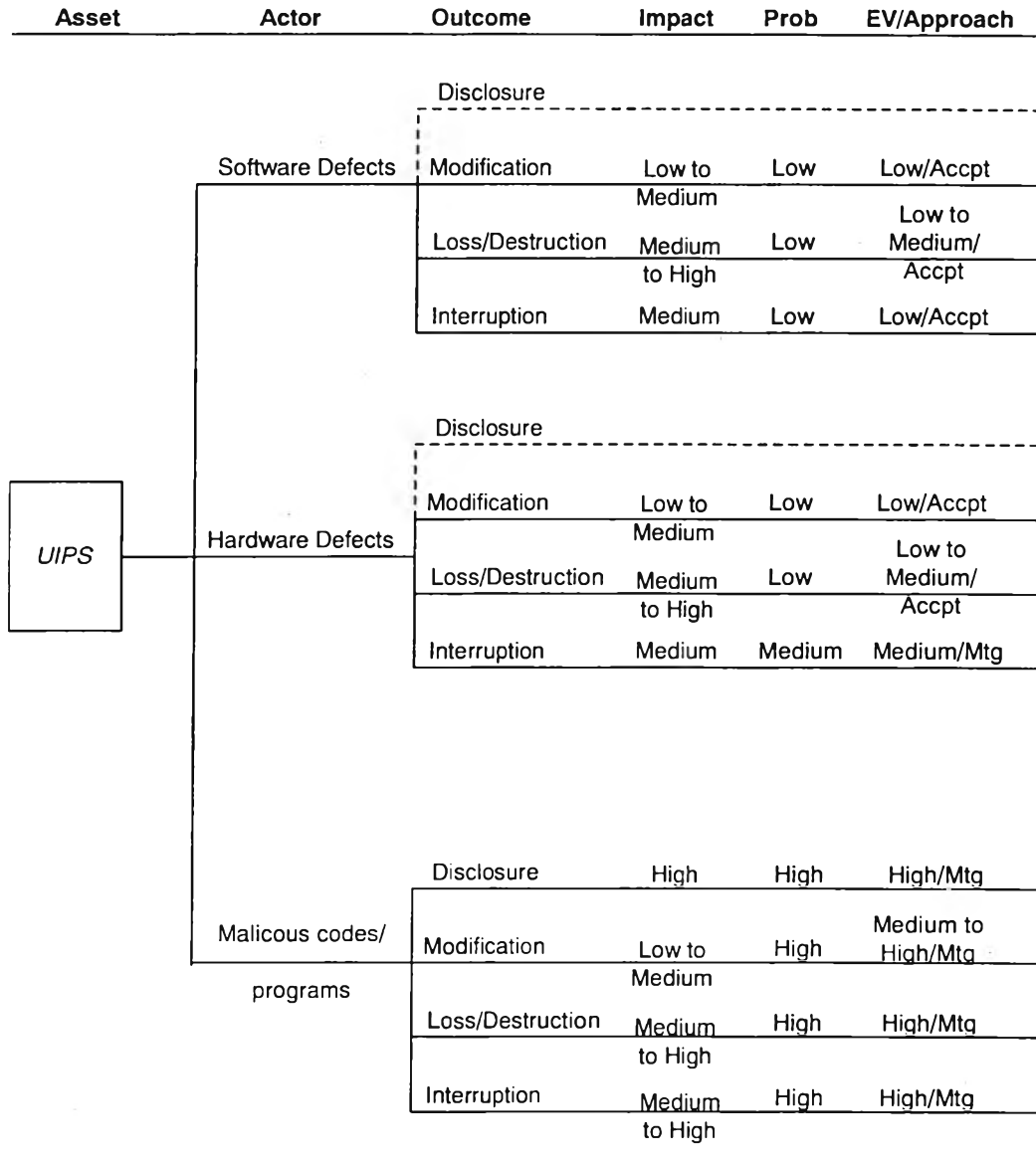

FIGURE C-7: *UIPS - Risk Profile for System Problem.*

APPENDIX C-8

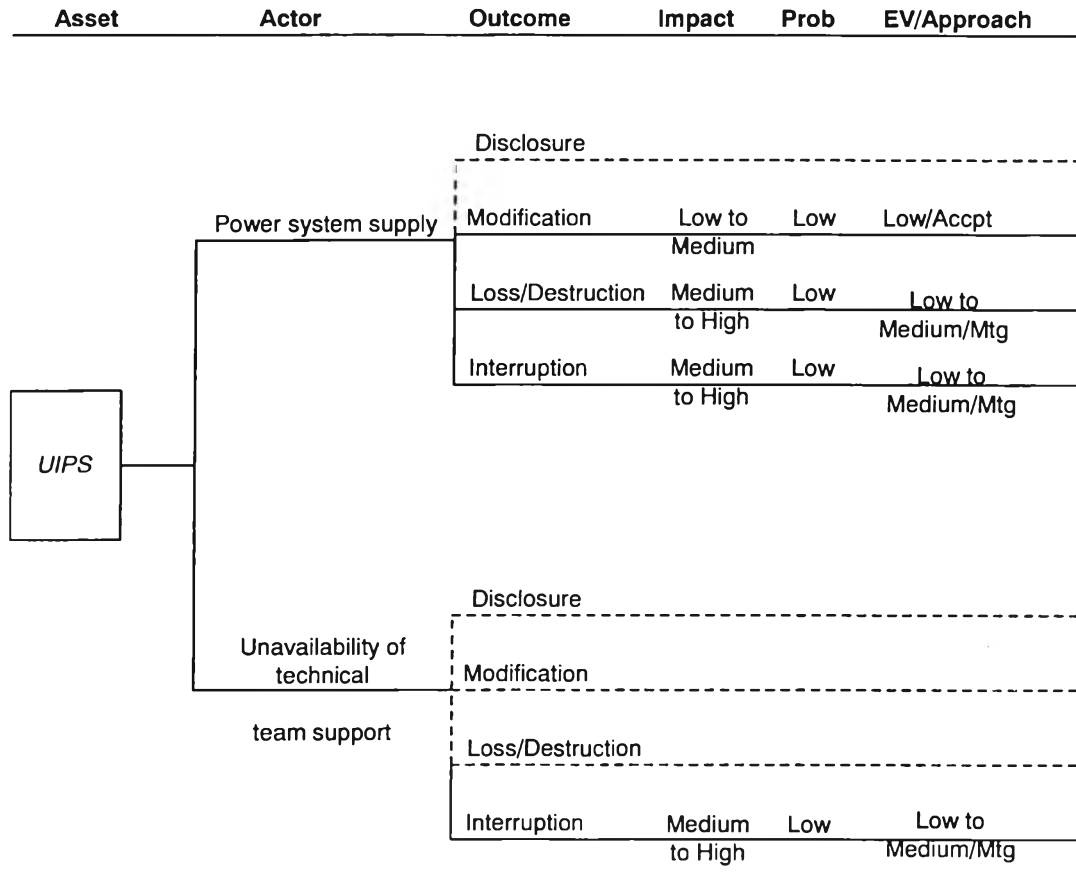

FIGURE C-8: *UIPS - Risk Profile for Other Problems.*

APPENDIX C-9

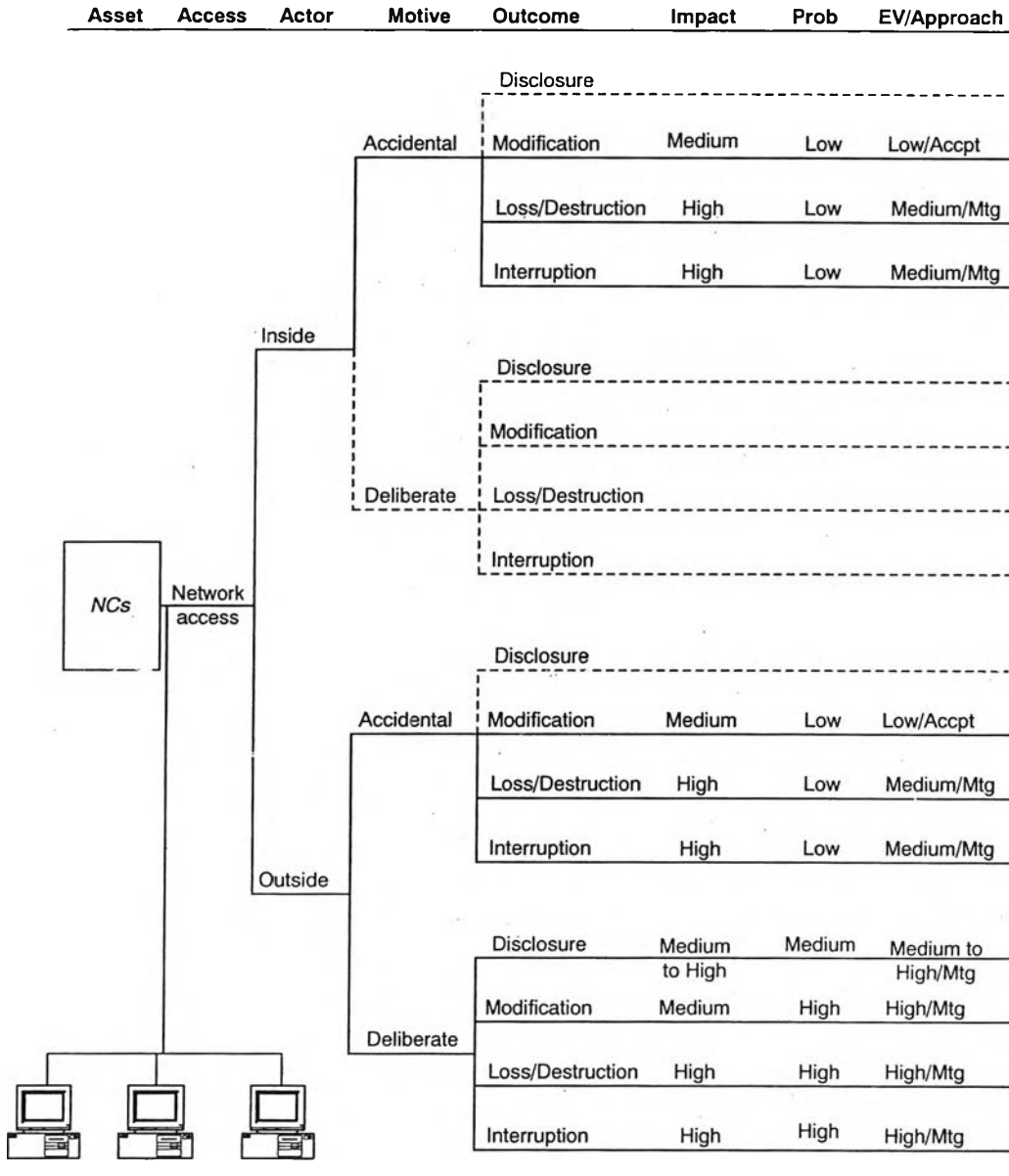

FIGURE C-9: *NCs - Risk Profile for Human actors using network access.*

APPENDIX C-10

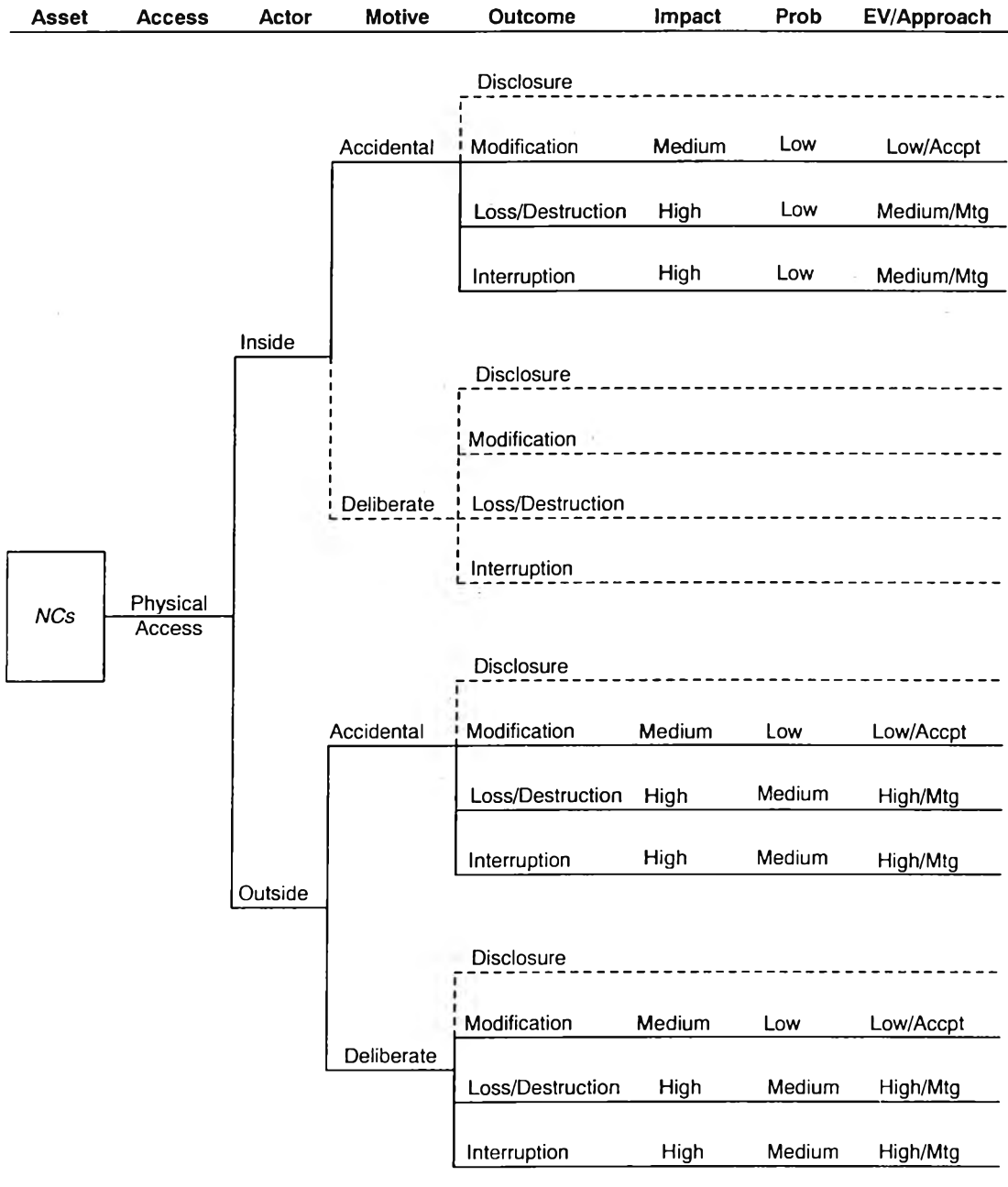

FIGURE C-10: *NCs - Risk Profile for Human actors using physical access.*

APPENDIX C-11

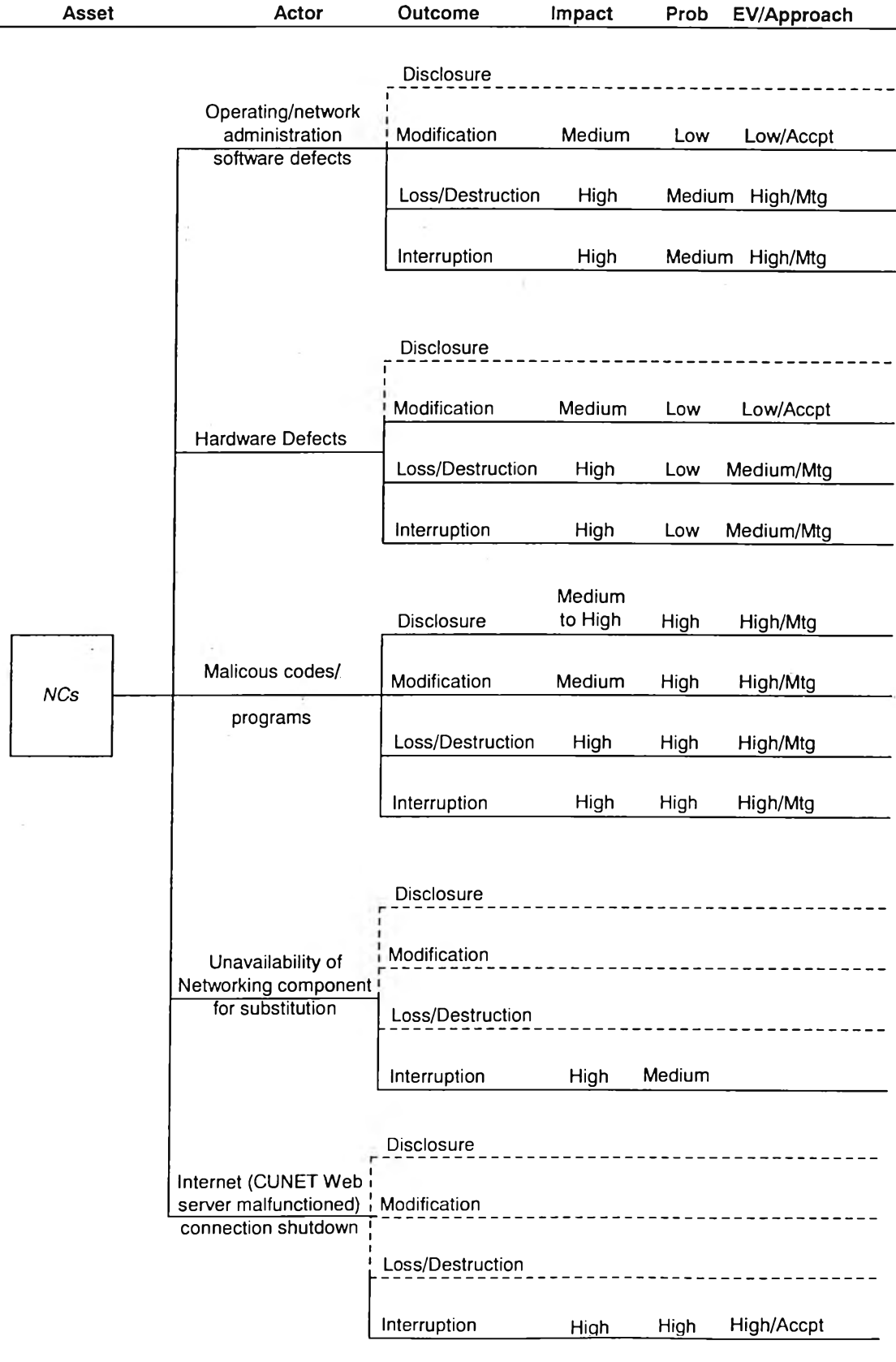

FIGURE C-11: *NCs - Risk Profile for System Problems.*

APPENDIX C-12

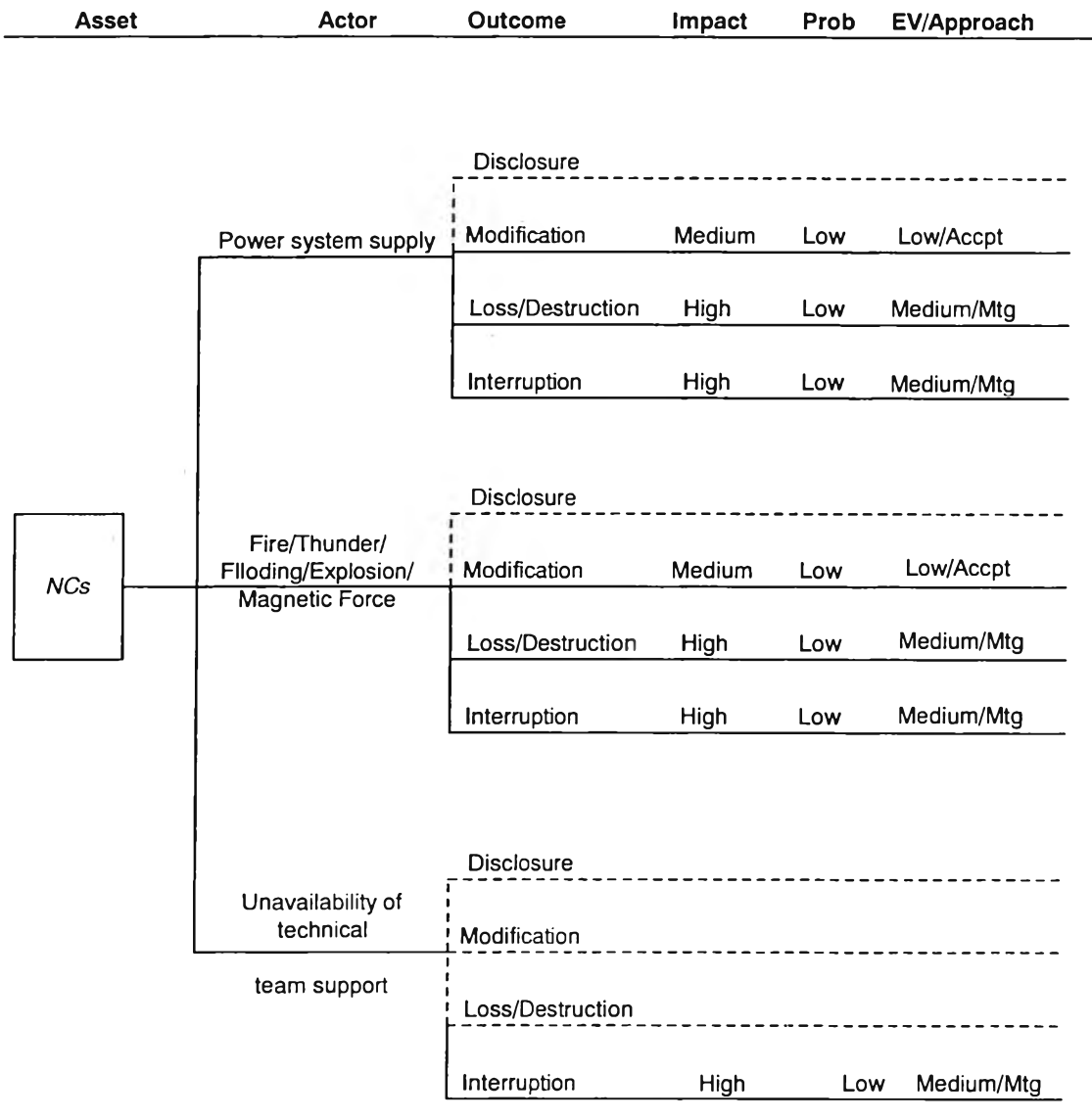

FIGURE C-12: *NCs - Risk Profile for Other Problems.*

APPENDIX C-13

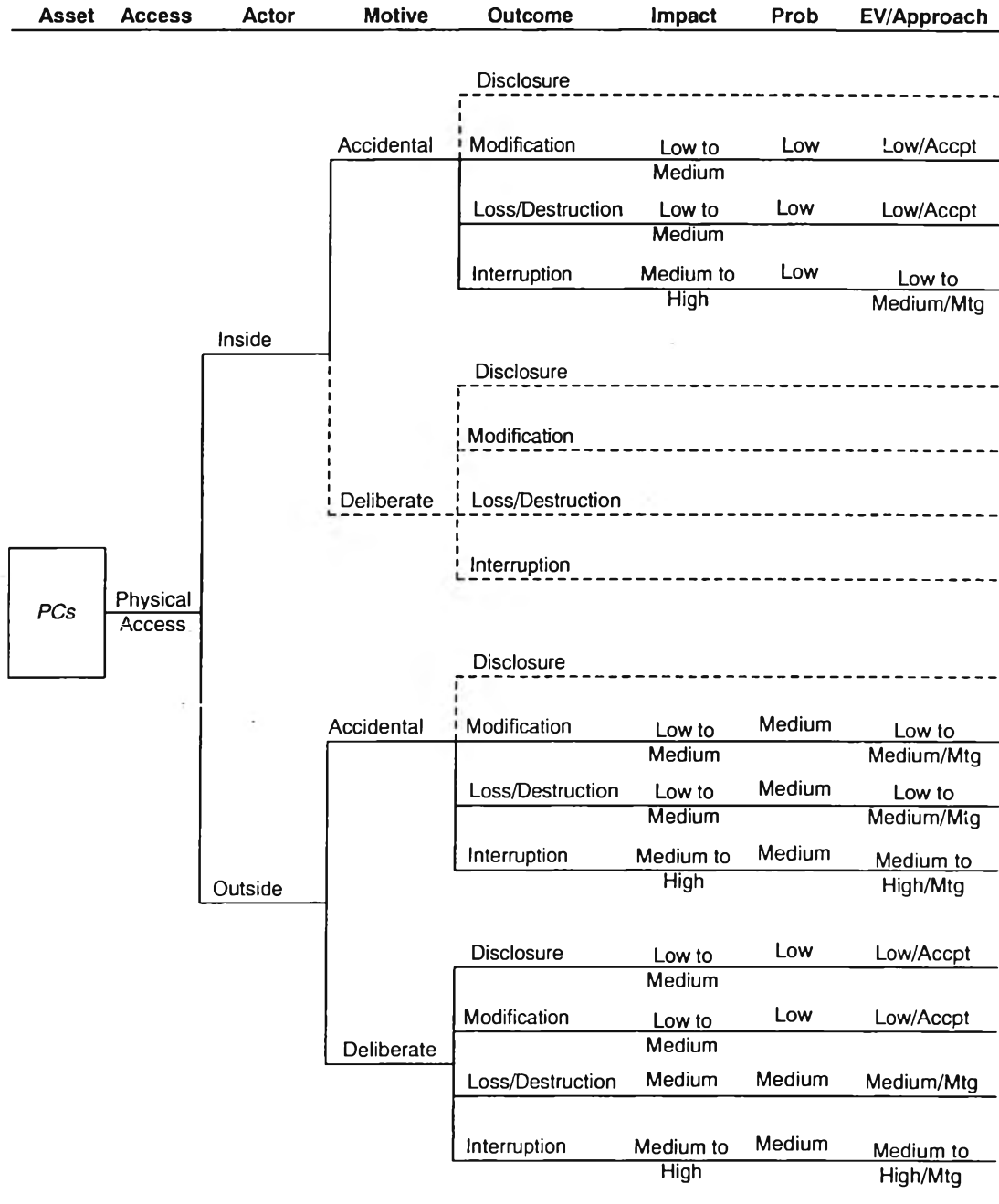

FIGURE C-13: *PCs - Risk Profile for Human Actors Using Physical Access.*

APPENDIX C-14

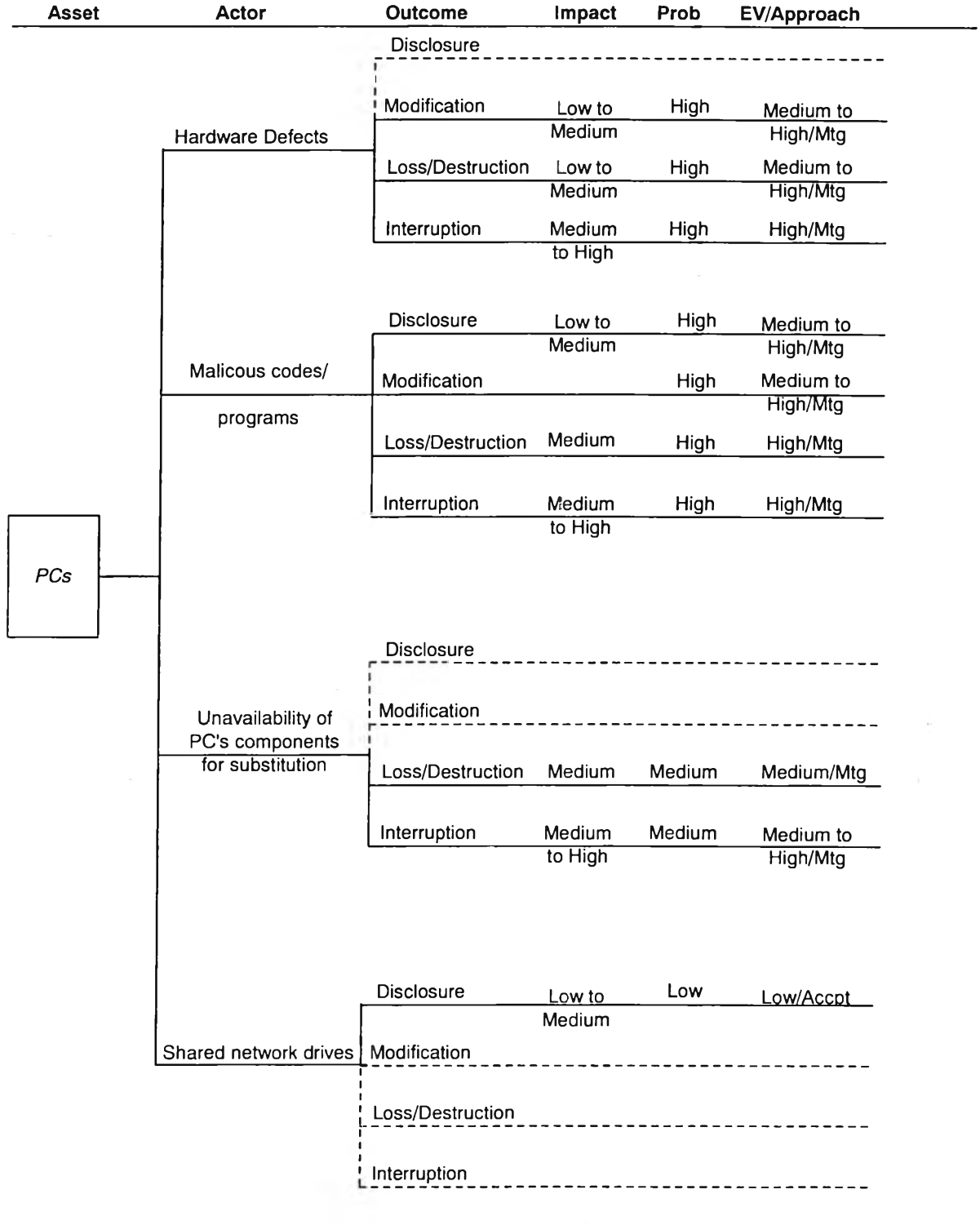

FIGURE C-14: *PCs - Risk Profile for System Problems.*

APPENDIX C-15

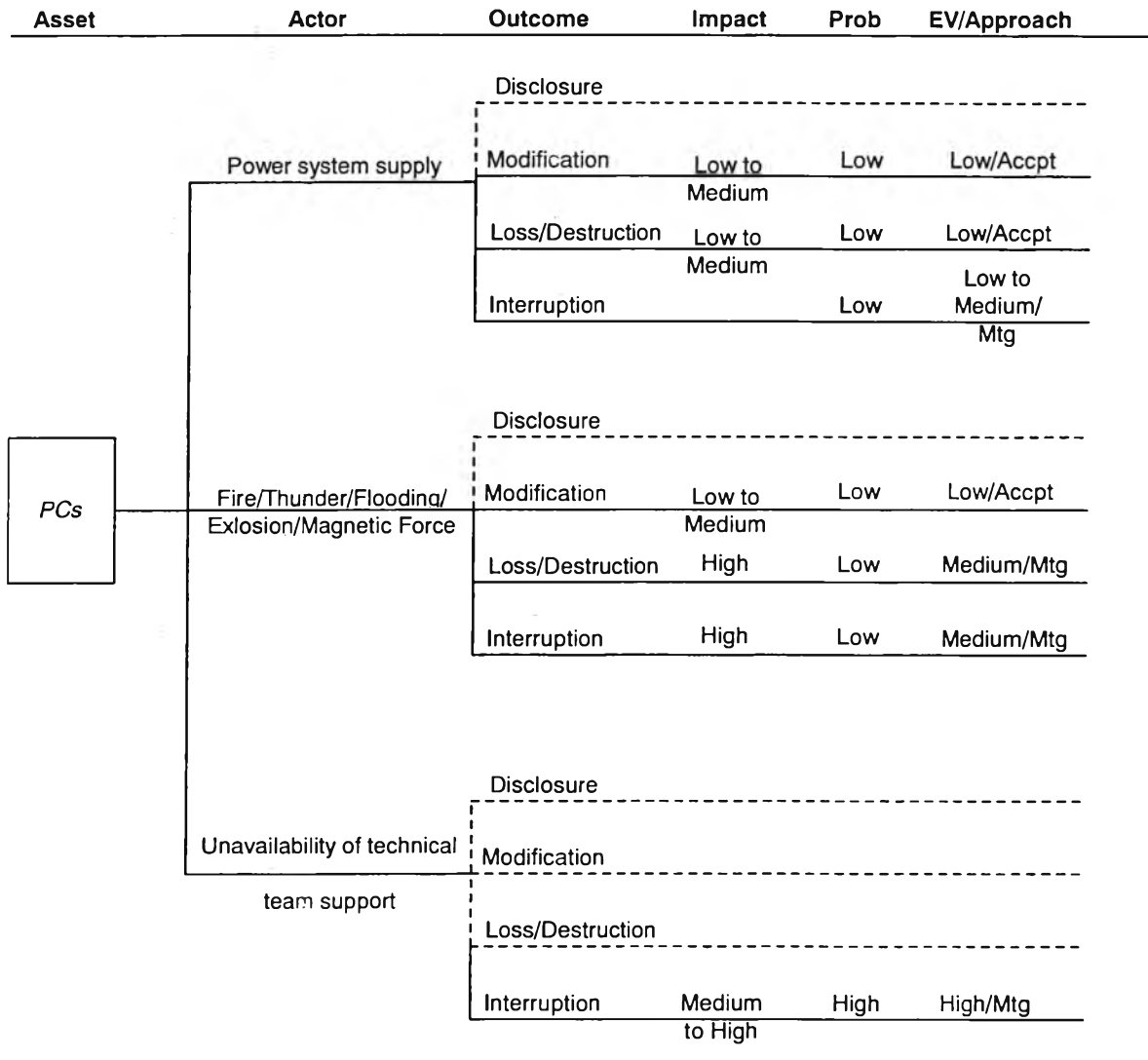

FIGURE C-15: *PCs - Risk Profile for Other Problems.*

APPENDIX C-16

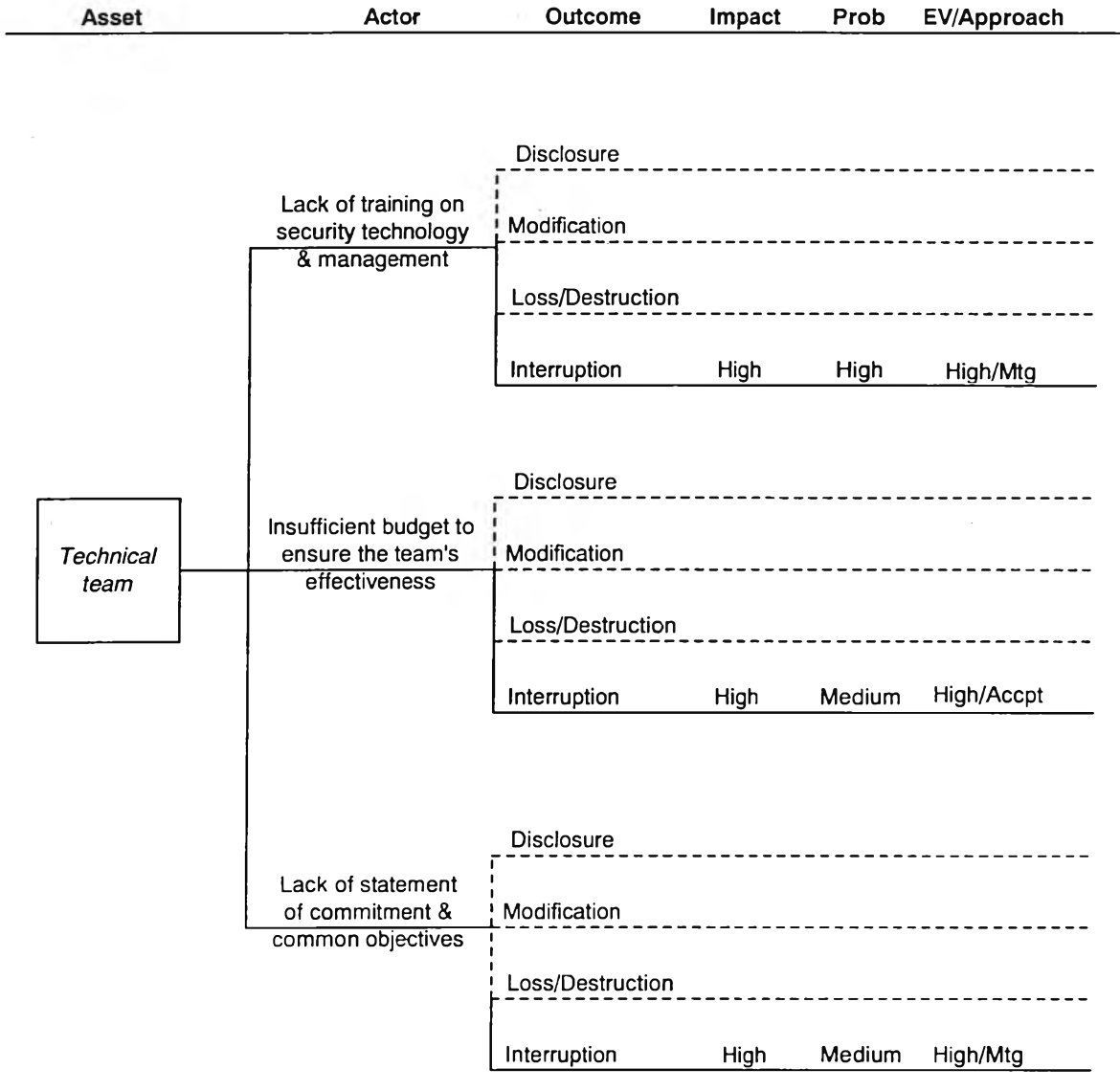

FIGURE C-16: *Technical team - Risk Profile for Other Problems.*

APPENDIX D

APPENDIX D

A -

Access: The ability to enter a secured area, and the process of interacting with a system. Used as either a verb or a noun.

Access authorization: Permission granted to users, programs, or workstations.

Access control: A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Audit: The independent collection of records to access their veracity and completeness.

Audit trail: An audit trail may be on paper or on disk. In computer security systems, it is a chronological record of when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.

Authenticate: In networking, to establish the validity of a user or a communications server.

Authentication: The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

Authentication tool: A software or hand-held hardware "key" or "token" used during the user authentication process. See *key* and *token*.

Authorization: The process of determining what number of activities is permitted. Usually, authorization is in the context of authentication. Once the user is authenticated, the user may be authorized different levels of access or activity.

B -

Business-critical applications: The vital software needed to run a business, whether custom written or commercially packaged, such as accounting or finance.

- C -

CERT: The Computer Emergency Response Team, established at Carnegie -Mellon University after the 1988 Internet worm attack named Morris.

Challenge/response: A security procedure in which one communicator requests authentication of another communicator and the latter replies with a pre-established appropriate reply.

Client/device: Hardware that retrieves information from a server.

Coded file: In encryption, a coded file contains unreadable information.

Computer security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

Computer security audit: An independent evaluation of the controls employed to ensure appropriate protection of an organization's information assets.

- D -

Data-driven attack: A form of attack that is encoded in innocuous-seeming data executed by a user or other software to implement an attack. In the case of firewalls, a data-driven attack is a concern because it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data encryption standard (DES): An encryption standard developed by EBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors.

Decode: Conversion of encoded text to plain text through the use of a code.

Decrypt: Conversion of either encoded or enciphered text into plain text.

Dedicated: A special-purpose device. Although capable of performing other duties, it is assigned to only one.

Defense in depth: The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

DES: Data encryption standard.

- E -

E-mail bombs: Code that when executed sends many messages to the same address for the purpose of using up disk space or overloading the e-mail or Web server.

Encryption: The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm).

Environment: The aggregate of external circumstances, conditions, and events that affect the development, operation, and maintenance of a system.

- F -

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

- G -

Gateway: A bridge between two networks.

Global security: The ability of an access-control package to permit protection across a variety of

mainframe environments, providing users with a common security interface to all.

- H -

Hack: Any software in which a significant portion of the code was originally another program.

Hackers: Those intent on entering an environment to which they are not entitled entry for whatever purpose (e.g., entertainment, profit, theft, prank), usually involving iterative techniques, escalating to more advanced methodologies, and use of devices to intercept the communications property of another.

- I -

IETF (The Internet Engineering Task Force): A public forum that develops standards and resolves operational issues for the Internet. IETF is purely voluntary.

Information systems technology: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction or the inability to process that information.

Insider attack: An attack originating from inside a protected network.

Internet: A web of different, intercommunicating networks funded by both commercial and government organizations. The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of open networks in the late 1980s required a new model of communications. The amalgamation of many types of systems into mixed environments demanded a better translator between these operating systems and a nonproprietary approach to networking in general. Telecommunications Protocol/Internet Protocol (TCP/IP) provided the best solutions.

Intrusion detection system: A system dedicated to the detection of break-ins or break-in attempts manually either via software expert systems that operate on logs or other information available on the network.

ISO (International Standards Organization): Sets standards for data communications.

ISSA: Information Systems Security Association.

- K -

Key: In encryption, a sequence of characters used to encode and decode a file. One can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, which is a device used to send and receive challenges and responses during the user authentication process. Keys may be small,

hand-held hardware devices similar to pocket calculators or credit cards or they may be loaded onto a PC as copy-protected software.

L -

Local area network (LAN): An interconnected system of computers and peripherals; LAN users share data stored on hard disks and can share printers connected to the network.

Logging: The process of storing information about events that occurred on the firewall or network.

Log processing: How audit logs are processed, searched for key events, or summarized.

Log retention: How long audit logs are retained and maintained.

N -

Network computer (NC): A "thin" client hardware device that executes applications locally by downloading them from the network. NCs adhere to a specification jointly developed by Sun, IBM, Oracle, Apple, and Netscape. NCs typically run Java applets within a Java browser or Java applications within the Java Virtual Machine.

Network computing architecture: A computing architecture in which components are dynamically downloaded from the network into the client device for execution by the client. The Java programming language is at the core of network computing.

Network worm: A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability, or availability. A network worm may attack from one system to another by establishing a network connection. The worm is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

O -

One-time password: In network security, a password issued only once as a result of a challenge response authentication process. Cannot be "stolen" or reused for unauthorized access.

Operating system: System software that controls a computer and its peripherals. Modern operating systems, such as Unix, Linux, and Windows XP handle many of a computer's basic functions.

Orange book: The Department of Defense Trusted Computer System Evaluation Criteria. It provides information to classify computer systems, defining the degree of trust that may be placed in them.

P -

Password: A secret code assigned to a user, known by the computer system. Knowledge of the password associated with the user ID is considered proof of authorization. (See One-time password.)

Performance: A major factor in determining the overall productivity of a system, performance is primarily tied to availability, throughput, and response time.

Perimeter-based security: The technique of securing a network by controlling access to all entry and exit points of the network.

Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Private key: The element of a public/private key pair that is kept secret by the key pair owner. The private key is used to decrypt messages that have been encrypted by the corresponding public key. It also is used to construct a digital signature – the document to be signed first is hashed using a secure hash algorithm; then encrypting the hashed value using the private key forms the digital signature.

Public key: The element of a public/private key pair that can be known by anyone. The public key is used to encrypt information that is to be intelligible only to the holder of the corresponding private key. It also is used to decrypt a digital signature in order to compare the decrypted digital signature and the hashed value of the signed document.

R -

Remote access: The hookup of a remote computing device via communications lines, such as ordinary phone lines or wide area networks, to access network applications and information.

Risk analysis : The analysis of an organization's information resources, existing controls, and computer system vulnerabilities. It establishes a potential level of damage in dollars or other assets.

Rogue program: Any program intended to damage programs or data. Encompasses malicious Trojan horses.

S -

Server: The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

Server-based computing: An innovative, server-based approach to delivering business-critical applications to end-user devices, whereby an application's logic executes on the server and only the user interface is transmitted across a network to the client. Its benefits include single –point management, universal application access, bandwidth-independent performance, and improved security for business applications.

Social engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user to attempt to gain illicit access to systems.

T -

Trojan horse: (1) Any program designed to do things the user of the program did not intend to do or that disguise its harmful intent. (2) A program that installs itself while the user is making an authorized entry, and then is used to break in and exploit the system.

U -

User: Any person who interacts directly with a computer system.

User ID: A unique character string that identifies a user.

User identification: User identification is the process by which a user identifies herself to the system as a valid user—as opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system.

User interface: The part of an application that the user works with. User interfaces can be textdriven, such as DOS, or graphical, such as Windows.

V -

VPN (virtual private network): A private connection between two machines that sends private data traffic over a shared or public network, such as the Internet. VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies.

Virtual network perimeter: A network that appears to be a single protected network behind firewalls, but actually encompasses encrypted virtual links over untrusted networks.

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

W -

WLAN (wireless local area network): A wireless Network that corresponds to wireless laptops.

BIOGRAPHY

Name: Khuong Le Nguyen

Year of Birth: 10 September 1975

Qualification:

Civil Engineering (Hochiminh City University of Technology – Vietnam): 93-98

Computer Engineering (NUS – Singapore): 98 – 2001

Master of Civil Engineering (University of Liege – Belgium): 2001 – 2002

Organization: The "HUT-TODAI" program – a long term educational project co-operated between Hochiminh City University of Technology (HCMUT - Vietnam) and the University of Tokyo (TOU – Japan).