Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®
Computer Standards & Interfaces 26 (2004) 501–513
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

A study on information security management system evaluation—assets, threat and vulnerability

Kwo-Jean Farn[a,b,*], Shu-Kuo Lin[a], Andrew Ren-Wei Fung[a,c]

[a] *Institute of Information Management, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan, ROC*
[b] *Internet Security Solutions International Co., Taiwan, ROC*
[c] *DCGS for Communications, Electronics and Information (J-6), Ministry of National Defense, Taiwan, ROC*

Received 1 October 2003; received in revised form 11 March 2004; accepted 20 March 2004
Available online 28 April 2004

Abstract

The security of information system is like a chain. Its strength is affected by the weakest knot. Since we can achieve 100% Information Security Management System (ISMS) security, we must cautiously fulfill the certification and accreditation of information security. In this paper, we analyzed, studied the evaluation knowledge and skills required for auditing the certification procedures for the three aspects of ISMS—asset, threat, and vulnerability.

Keywords: Certification; Evaluation; Framework; Information Security Management System; National Information Assurance Certification and Accreditation Process

1. Introduction

The Executive Yuan of Republic of China (Taiwan, ROC) is the highest administration unit in the country. The Chief of the Executive Yuan is like a premier in France. The "National Information and Communication Initiative Committee" (NICI) of the Executive Yuan is in the process of promoting all the related information security tasks. It was reported that NICI has forbidden the government and educational institute to use the software "Fluxay". For "Fluxay", a product by Banyet Soft Labs in China might steal and fetch information from the end-users back to China, which causes the security problems [1]. The design of "Fluxay" is very efficient; it uses Dictionary Attack Method, detecting port 2049(NFS), port 137(NETBIOS), port 80(WWW), port 79(FINGER), port 43(WHOIS), port 25(SMTP), port 21(FTP Control), etc. until it finds the correct password, and then intrude the computer automatically. In other words, "Fluxay" can be classified as "automatic machine gun" in traditional weapons similar to the "digital weapon" for UNIX system in Table 1.1 There is no clear evidence whether "Fluxay" will really fetch the information from the end-users to the designated website. On August 1, 2002, there was a headline "Hackers in China Attacking, NICI gave Warning" in United Daily Newspaper [2]. Similar news reporting

* Corresponding author. Institute of Information Management, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan, ROC. Tel.: +886-3-5712301; fax: +886-3-5723792.
E-mail address: kuo@iim.nctu.edu.tw (K.-J. Farn).

0920-5489/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2004.03.012

Table 1.1
India Nuclear Explosion Research Event in May of 1998

Item	Event
1	In May 1998, a 15-year old US lad, nicknamed "t3k-9", was extremely angry possibly because of humanity reasons or being sorry over the "poverty of the Third World poor peoples" or some other unknown reasons.
2	t3k-9 hooked into Infoseek search engine, connected with ".in atomic" and found Bhabha Atomic Research Center (BARC) of India; he clicked on BARC and attacked with "John Ripper DES Encryption Cracker", and in 45 s t3k-9 found himself becoming a legitimate BARC user.
3	A few days later, t3k-9 released the whole password file (of about 800 legitimate users) on hackers' channel. BARC suffered hundreds of hacker attacks.

are as follows: Taiwan Coalition Party announcer Mrs. Hsia held a press conference indicating there has been many Mainland China hackers intruding Taiwan's websites, such as the Taiwan Awareness Forum in the Taiwan's Tea Party website. From the host's record, it was found the source of the hacker could be traced to the website of Kaohsiung City Council, Taiwan. The above incidents actually are the crackers' tricks to attack the end-users indirectly. Starting in 1995, these hacker groups on the websites have provided the Chinese instructions to search for end-users' weak spots, using the trapdoors to break the systems [3,4]. In Taiwan, many people have not formed a habit of a secure coding according to information security technology rules. Using the "Fluxay" and other utility programs, 5–10% of websites in Taiwan are intruded and the users are not aware of it.

It was estimated that there are about 15 bugs in each 1000 lines of coding program. So in the Windows 2000, which is about 500,000,000,000 lines of coding, there should be 750,000 bugs. In January 2002, the president of Microsoft, Bill Gates, announced: "The security and privacy of all the software products are far more important than any other new functions." Later, in February 2002, Microsoft sent 7000 systems programmers for special security training. The company openly declared "An establishment of a confidential information system war, "claiming" doing the best to provide security information products as secure as the service from electric company, water company, and telecommunication." In the future, the utility tools such as "Fluxay" will still cause security problems as in the case of "t3k-9" (Table 1.1) in the digital world. That is why National Security Agency (NSA) insisted that the auditing of Information Security Management System (ISMS) should be done in a technologically secure information [5–9].

In 2003, the NICI had demanded the certification for any ISMS. Our government has not set up the ISMS self-assessment as the U.S. government [5]. On November 28, 2000, the Security, Privacy and Critical Infrastructure Committee of National Institute of Standards and Technology (NIST) proposed a Federal Information Technology Security Assessment Framework (FITSAF). In the FITSAF, there are five levels of ISMS [5]. If the level of ISMS in FITSAF is below 3, there is more chance for the hacker's intrusion. Ever though the audit log is complete, or it passes the BS 7799-2:2002 certification, the system is still vulnerable [5–9]. If our government can also do the self-evaluation based on the security self-assessment, Guide for Information Technology Systems, NIST SP 800-26, FITSAF and perform the information system technology security Gap Analysis, the results would be more valuable. In 1999, Common Criteria (CC) for information products/systems security evaluation as an international standard was formally issued. However, with the increasing diversity of threats, in addition to the solution on engineering side, an establishment of a complete education training, the verification and validation of Penetration Test, the security evaluation of certification and accreditation are all required, which are also the targets of level 4 or level 5 in FITSAF. Especially, on July 31, 2002, when NICI issued the warning, they have to count on "Penetration Test" and ISMS auditing. In fact, how to prevent such attacks becomes a cornerstone of the establishment of the ISMS.

In May 2003, the Technical Committees (TC) 11 of International Federation for Information Processing (IFIP) held an annual convention. Control items and protection classes and their relationships were proposed as in Table 1.2 [10]. In Section 2, we introduce the U.S. National Information Assurance Certification and Accreditation Process (NIACAP) guide; in Section 3, based on the U.S. NIACAP pioneer project, we analyze the framework of the ISMS. Finally, we propose some required knowledge

Table 1.2
The relationship of control items and protection classes to ISO/IEC 17799:2001(E)

ISO/IEC 17799:2001(E)control items	Protection class			
	1. Inadequate	2. Minimal	3. Reasonable	4. Adequate
1. Security policy	×	×		
2. Organizational security	×	×		
3. Asset classification and control	×	×		
4. Personnel security	×			
5. Physical and environment security	×			
6. Computer and network management	×			
7. Access control	×			
8. System development and maintenance	×	×		
9. Business continuity management	×	×		
10. Compliance	×	×		

Source: Eloff, M.M. and J.H.P. Eloff, Information Security Management System: Processes and Products, SEC 2003, Security and Privacy in the Age of Uncertainty, pp. 193–204, Kluwer Academic Publishers (2003).
Blank shows enhance control item for the processes and procedures of ISMS research.

and skills for the auditing of the ISMS, and make some conclusions.

2. The brief introduction of U.S. NIACAP

On December 5, 1990, the U.S. National Research Council released the report "Computers at Risk (CAR): Safe Computing in the Information Age". As indicated in the conclusion of the report [9], the individuals, business entities, and government agencies are under the far-reaching influence imposed by the information system as the global information era is approaching with no restrictions of time and distance. As a result, human beings will have to accept the information system as a part of their daily lives and depend on the continual advancement of information system. For instance, the increasing use of information system has not only changed the organizational structures and operational procedures fundamentally, but also modified the interaction methods inside the organizations. The existing operational procedures would cease to function and could not restore the previous working procedures if the information system malfunctions. The malfunctioning information system will affect the airline companies, securities trading, financial operations, medical service, and rapid transit systems tremendously; such influence is closely related to the public safety and thus justifies the importance of dependability. On the other hand, human beings benefit from their use of

Table 2.1
No. 11 Policy, U.S. National Security Telecommunications and Information Systems Committee (NSTISSP No. 11)

Item	Event
1	Issued by U.S. National Security Telecommunications and Information Systems Committee (NSTISSC) in accordance with National Security Directive No.42 (NSD-42) announced in July 1990.
2	Prior to announcing NSTISSP No. 11, NSTISSC announced NSTISSAM (Advisory Memorandum) INFOSEC/1-99 in March 3, 1999, and NITISSC announced NSTISSI (Instruction) No.1000 of National Information Assurance Certification and Accreditation Process (NIACAP).
3	The decree: (a) As of January 1, 2001, the information technology of the information infrastructure shall comply with the confirmation plan initiated by National Institute of Standards and Technology (NIST). (b) As of July 1, 2002, the rules stated in (a) shall be mandated in accordance with Presidential Decision Directive No. 63 (PDD-63).

These publications can be obtained from the NIST Computer Security Resource Center (http://www.csrc.nist.gov).

the information. Nevertheless, the information system is far from satisfactory with respect to the safety requirement. Ironically, no information system can tolerate the minimal defects or attack at the time that the public services, business activities, and the individuals are highly dependent on the less trustworthy information technologies.

CAR imposes an immediate and far-reaching influence. Based upon CAR, the US President ordered the implementation of information system security as a national goal, to be carried out by the National Institute of Standards and Technology (NIST) responsible for the "Standards and guidance". Working with the International Organization for Standardization (ISO) closely, NIST has announced nearly 30 Federal Information Processing Standards (FIPS), Information System Security Guidance, Planning Guidance, and Risk Management in the last 10 years. ISO announced the CC as the international standard with respect to the information technology security accreditation of the information products/systems in the turn of bicentennial (December 15, 1999) [10], and has requested the U.S. federal government to audit the information security and administration system internally in accordance with the NIST guidance announced in the last 10 years. The information security and administration system was divided into five levels in accordance with the maturity and integration of capabilities. Certification and accreditation were essential for third level and above. U.S. National Security Telecommunications and Information Systems Security Committee (NSTISSC) announced the decrees shown on Table 2.1, in July 2000, and requested all agencies to execute the tasks related to information technical certification and accreditation.

Based upon CC and the PUB (Publication) 140-2 [11] of Federal Information Processing Standard (FIPS) proclaimed on May 25, 2001, NIST announced the information technology certification and accreditation plan shown as Table 2.1 on October 28, 2002, to be discussed publicly and to be implemented in the spring of this year. The guidance documents are shown as Fig. 2.1 [12] with content shown as Table 2.2 [5–14]. Fig.

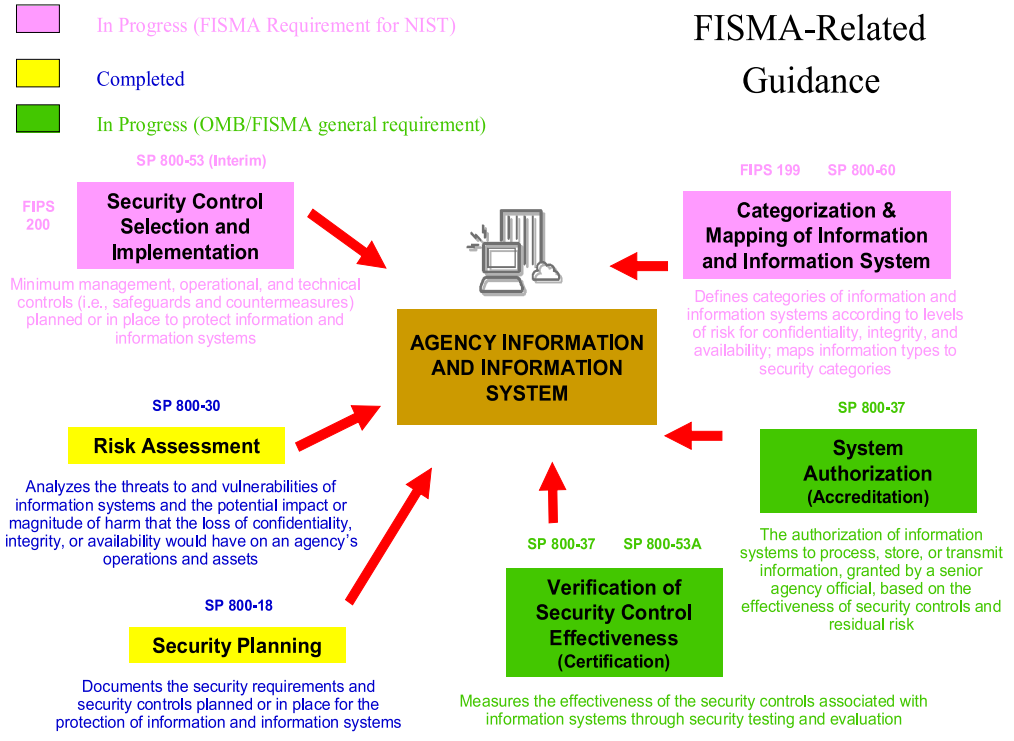


Fig. 2.1. U.S. Federal Information Security Management Act (FISMA) Certification and Accreditation Process Related Guidance.

Table 2.2
National Information Assurance Certification and Accreditation Process (NIACAP) of U.S. Federal Government

Item	Process contents
1	Initiation Phase:
	(a) Preparation
	(b) Notification and Resource Identification
	(c) Security Plan Analysis, Update, and Acceptance
2	Security Certification Phase:
	(a) Security Control Verification
	(b) Security Certification Documentation
3	Security Accreditation Phase:
	(a) Security Accreditation Decision
	(b) Security Accreditation Documentation
4	Continuous Monitoring Phase:
	(a) Configuration Management and Control
	(b) Ongoing Security Control Verification
	(c) Status Reporting and Documentation

Based on (a) U.S. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, announced by U.S. National Security Telecommunications and Information Systems Security Committee (NSTISSC) in April 2000, and (b) Federal Information Security Management Act (FISMA) announced in December 2002.

2.2 illustrates the relationship between NIST Special Publication 800-37 [7] and other special publications supporting the C&A process. These publications can be obtained from the NIST Computer Security Resource Center (http://www.csrc.nist.gov). The C&A process is shown as Table 2.3 with process content shown as Fig. 2.2.

According to the document that U.S. has announced, NIACAP performs product (/system/service) certification toward information security process through CC 2.1 and FIPS PUB 140-2. It also works on certification toward the systems of information technology on the basis of ISO/IEC 17799. The certification stage is responsible for whether the residual risk management, accepted by these three certification processes, is reasonable [7].

3. ISMS evaluation

Reducing risks is the target of ISMS protection mechanism as shown in Fig. 3.1 [15]. In order to achieve the ISMS, as early as in 1998, NIACAP started a Pilot Project, which accomplished the ISMS assurance ranging from national defense telecommunication, to finance infrastructure et al. as shown in Fig. 2.2. Table 3.1 illustrates the input and output for each stage. The telecommunication infrastructure of the U.S. is a good example. Federal Aviation Administration (FAA) was founded in 1958, and was incorporated into Department of Transportation (DoT) in 1967. On February 21, 1996, FAA according to the Guideline for Computer Security Certification and Accreditation developed by NIST on September 29, 1983, announced the FAA automatic information system and communication security function requirement, and also demanded the information assurance as described in Fig. 3.2. In May 1998, FAA developed the FAA Telecommunication Infrastructure (FTI) information assurance for FAA itself as described in Fig. 3.2 and scope of FTI Security Services described in Fig. 3.3. In September of 2000, the version 1 of the FTI security guidelines incorporated the concepts of Basic Security Service and Enhanced Security Service and the ISO/IEC 21827 ISMS assessment model, which combines both the CC and the System Security Engineering Capability Maturity Model (SSE-CMM) [5–19].

Based on the relationships among the asset, threat, and vulnerability shown in Fig. 3.1, CC has proposed the relationship of security objectives for the TOE (Target of Evaluation) and security functional requirements in Fig. 3.4. The security functional requirements and security assurance requirements can provide the proper protections for the ISMS vulnerability and threat. Regarding the operational environment, the CC can, under certain assumption, fulfill the protection requirement for organizational security policies [10,12,20], and combines the requirements of information asset control in BS 7799-2:2002 [21], we proposed the framework of ISMS in Fig. 3.5, and the specification of TOE in Fig. 3.6. We emphasize respectively the management of the weakness of the information asset operation, the configuration management of the weakness of the information system threats. We also emphasize the function accuracy of the weakness of the information vulnerability. The main parts of the TOE summary specification are illustrated in Fig. 3.6. Based on the CC and through appropriate protection mechanism, reduction of ISMS threats, reduction of possibility of vulnerability, and the reduction of probability of the ISMS asset exposure, we build a solid ISMS.

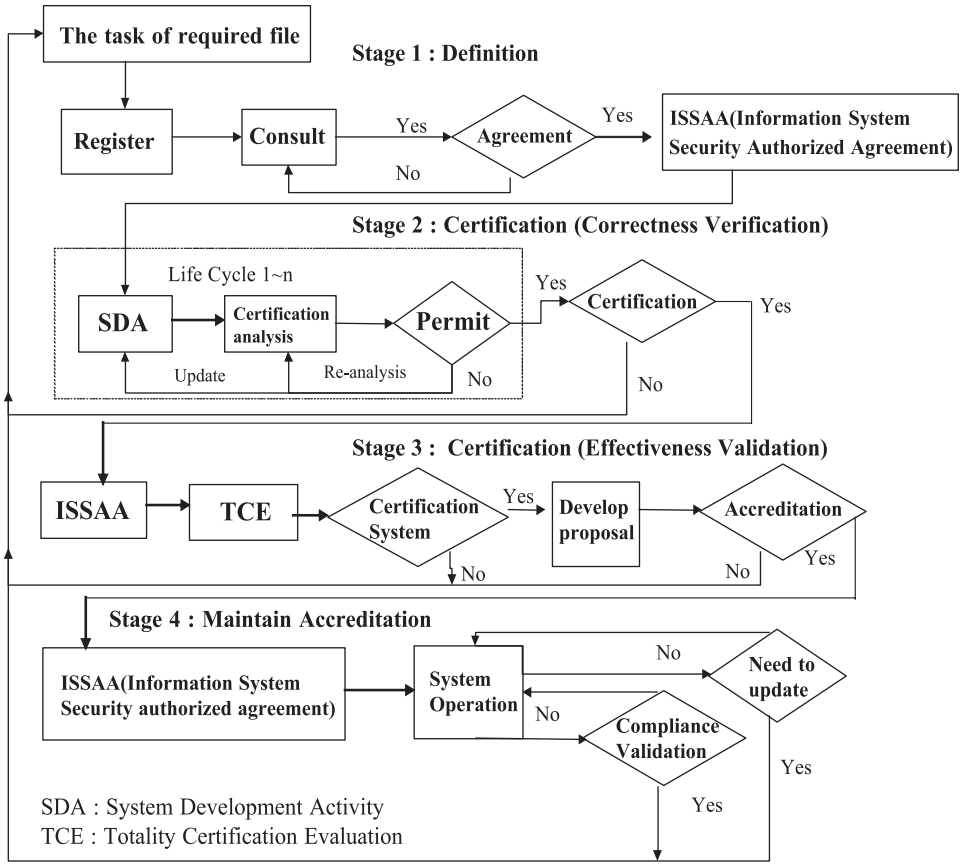


Fig. 2.2. U.S. National IT security assurance of process procedure.

The purpose of NIACAP is to achieve the target of Information Assurance: Information Operation (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration

Table 2.3
Scope of application for the standards related to IT security assurance framework [13]

Phase	Design/Implementation	Integration/Verification	Development/Transition	Operation
Approach				
Product [/system/service]	ISO/IEC 14598			PT
	ISO/IEC 15288	ISO/IEC 15288	ISO/IEC 15288	ISO/IEC 15288
	ISO/IEC 15408	ISO/IEC 15408	ISO/IEC 15408	ISO/IEC 15408
Process	ISO/IEC 21827	ISO/IEC 21827	ISO/IEC 21827	ISO/IEC 21827
	ISO/IEC TR 5504	ISO/IEC TR 15504	ISO/IEC TR 15504	ISO/IEC TR 15504
		ISO/IEC TR 13335	ISO/IEC TR 13335	ISO/IEC TR 13335
				ISO/IEC 17799
Environment	ISO 9000	ISO 9000	ISO 9000	ISO 9000
[/Organization/Personnel]	CISSP	CISSP	CISSP	CISSP

Certified Information System Security Professional (CISSP).
Penetration Testing (PT).

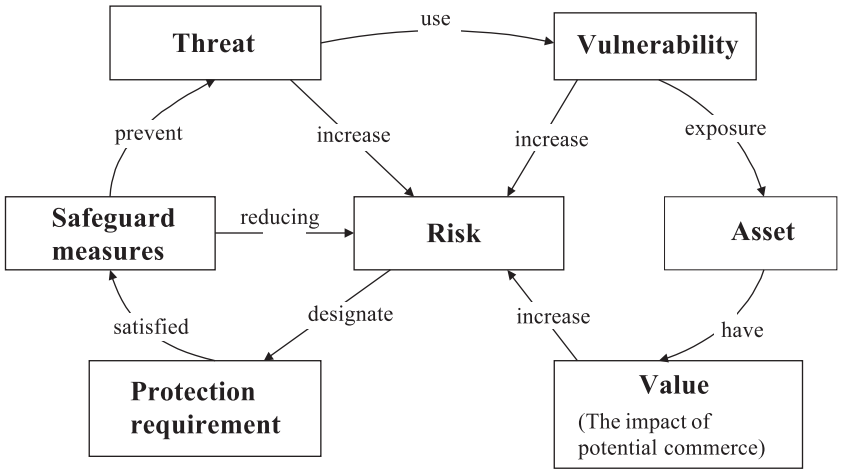


Fig. 3.1. ISMS risk component flowchart and relationship (ISO/IEC TR 13335-1). Note: Service Delivery Point (SDP).

of information systems by incorporating protection, detection, and reaction capabilities. Owing to the risk of vulnerability, threat of weakness exposure existed in information and information system lifecycle, CC 2.1 can provide the certification requirement of information technology Target of Evaluation (TOE) and the security target of developing environment, as shown in Fig. 3.4. NIACAP incorporates the certification of information security management system [22] of BS 7799-2:2002 as indicated in Fig. 3.5 and Fig. 3.6, and is likely to set up the evaluation process of IT integrity and the management of information system security certification mechanism, as illustrated in Fig. 3.7.

Table 3.1
Description of the Common Criteria for Information System lifecycle

Information System lifecycle stage	CC extra work action (Note: ISO/IEC 15408 also means CC)
Requirement analysis	(a) PP (Protection Profile)
	(b) APE (Assurance PP Evaluation)
Design (Definition stage)	(a) ST (Security Target)
	(b) ASE (Assurance ST Evaluation)
Development (Verification stage)	(a) TOE (Target of Evaluation)
	(b) Configuration Management Assurance
	(c) Delivered and Revolution Assurance
Verify (Verification stage)	(a) Testing Assurance
	(b) Vulnerability Assessment Assurance
Confirm (Validation stage)	(a) Delivered and Revolution Assurance
	(b) Guidance Text file Assurance
Operation and maintenance (Accreditation stage)	(a) Lifecycle Support Assurance
	(b) Vulnerability Assessment Assurance

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation.

4. Conclusion

With the quick development of information technology, personal computers, telecommunication, and the internet, people can access the information at any place, at any time. Though most of people acquire the information legally, some hackers have been trying to bypass the security loophole and attack the computer systems. The attack could come from either the external or the internal organizations. The attack can either be Denial of Service (DoS) or be big damage of the whole framework. The concept of information security has become a big issue for the whole world.

The purpose of ISMS is to assure the legal gathering of information resources and to provide complete, uninterrupted information system operation even when facing the intrusion. The design, implementation and operation of ISMS should pre-

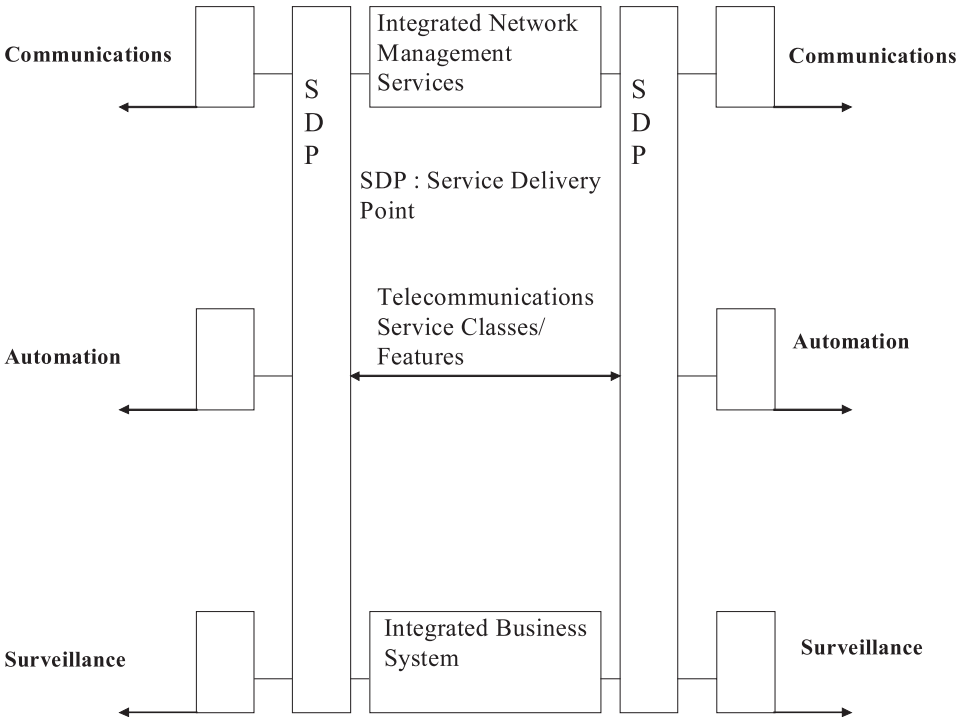


Fig. 3.2. FAA Telecommunication Infrastructure (FTI) functional architecture.

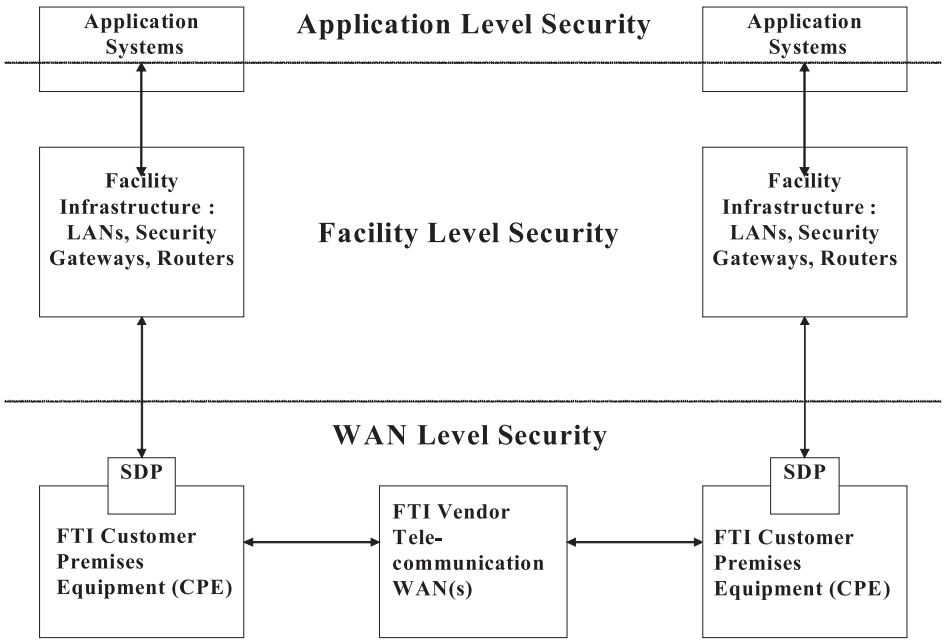


Fig. 3.3. Scope of FAA Telecommunication Infrastructure (FTI) Security Services.

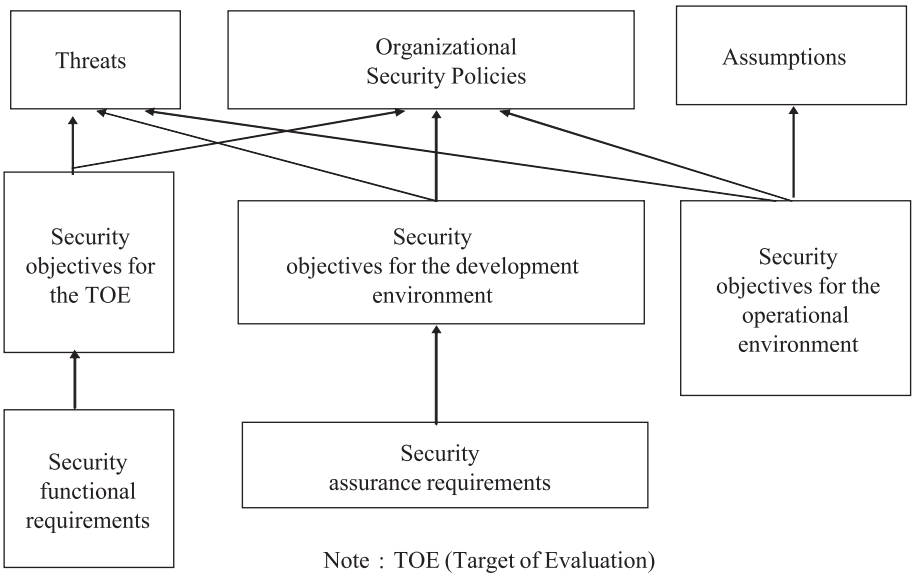


Fig. 3.4. Relationship between security objectives and requirements.

vent the hardware, software and users' data from being threatened externally and internally. The scope could range from the Key Management Mechanism to the complicated Access Control Mechanism. When dealing with these mechanism, the Risk Management should be considered. The balance of vulnerability and the threatening are also included in Risk Management [23].

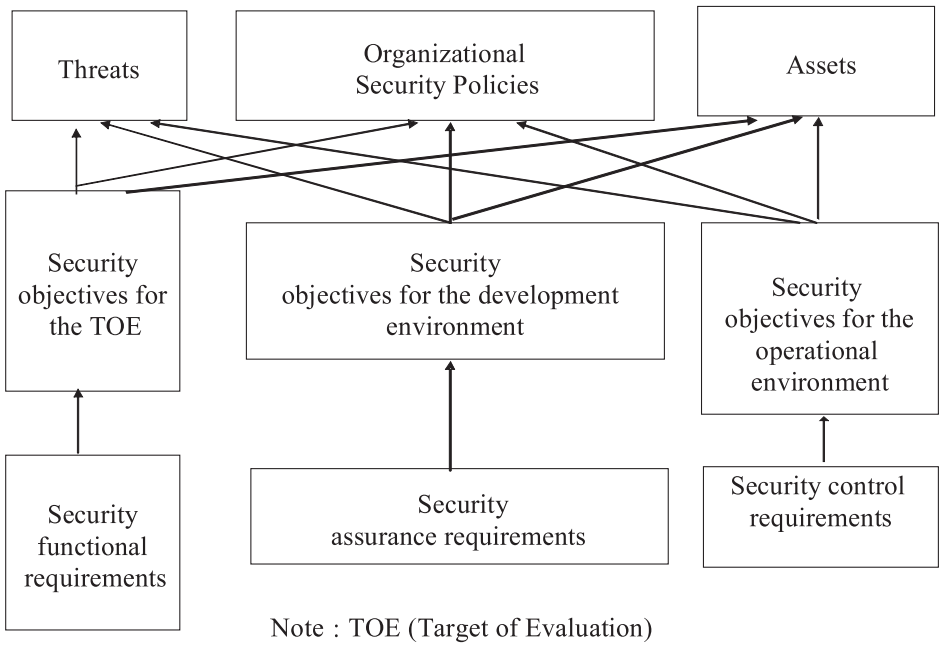


Fig. 3.5. Framework of Information Security Management System (ISMS).

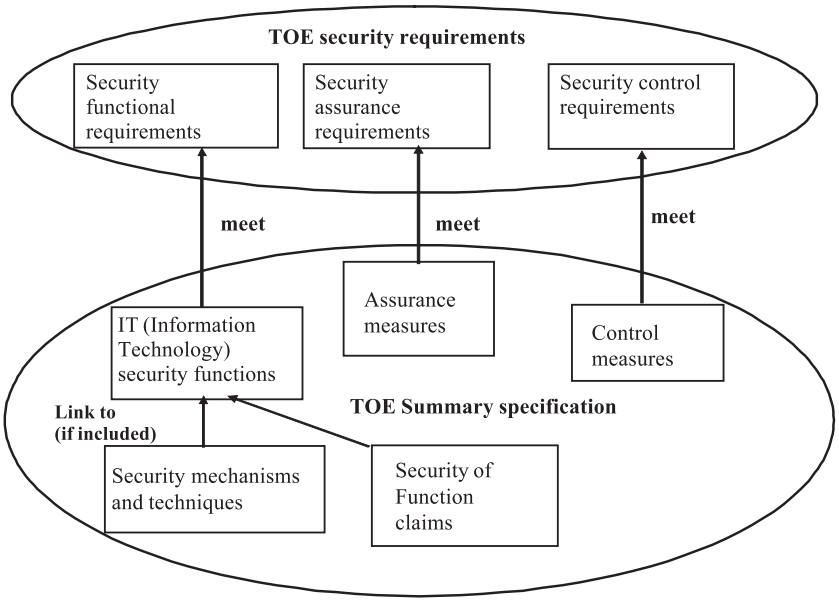
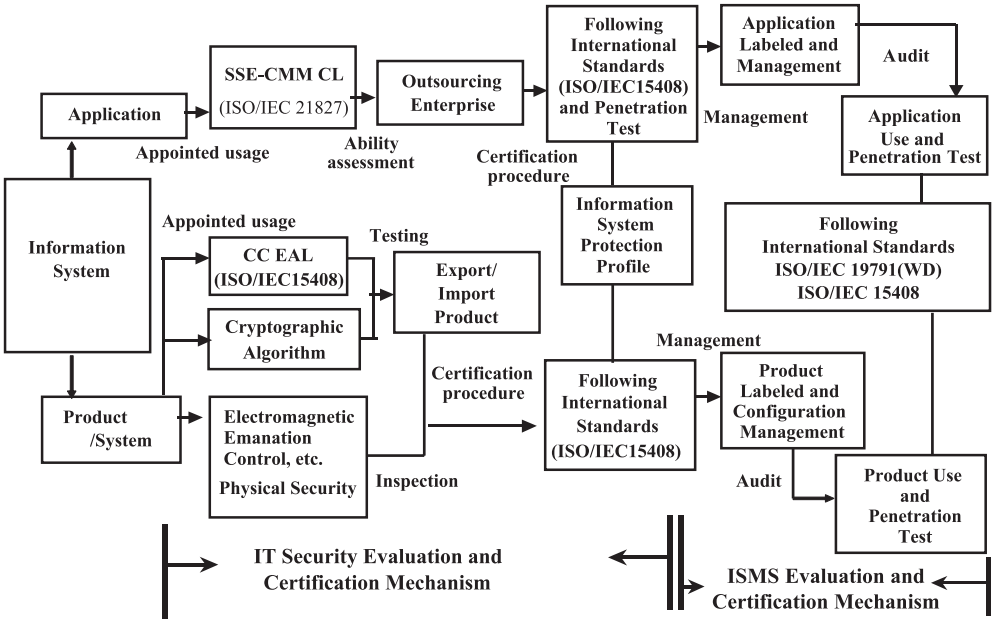


Fig. 3.6. Summary specification of ISMS Target of Evaluation (TOE).



Capability Level (CL).
Evaluation Assurance Level (EAL).

Fig. 3.7. Operation of the information system security certification mechanism.

Table 4.1
Lists of ISO/IEC JTC1/SC27 WG3 (Security Evaluation) have been announced and working on plans

1. ISO/IEC 15292 (2001-12-15): Protection Profile Registration Procedures.
2. ISO/IEC 15408 (1999-12-01): Evaluation Criteria for IT Security.
3. ISO/IEC TR 15443 (PDTR): A Framework for IT Security Assurance.
4. ISO/IEC TR 15446 (PDTR): Guide for the Production of Protection Profiles and Security Targets (PPST Guide).
5. ISO 18045 (WD): Methodology for IT Security Evaluation (CEM).
6. ISO/IEC 19790 (WD): Security Requirements for Cryptographic Modules.
7. ISO/IEC 19791 (WD): Security Assessment of Operational Systems.
8. ISO/IEC 19792 (WD): A Framework for Security Evaluation and Testing of Biometric Technology (SETBIT).
9. ISO/IEC 21827 (2002-10-01): Systems Security Engineering-Capability Maturity Model (SSE-CMM).

To protect the security of information asset is considered to be the common agreements among modern civilized countries and the indispensable cultivation of democratic countries, societies, and citizens. However, the human nature is not always good, and it is common for its guardians to intrude the security of the asset. Information security management not only is related to the ''public security'', but also takes the organization levels, evil-disposed outsiders, and burglars inside the company into consideration. Compared with the environment management system and industry sanitation security, its certification is much more difficult. The issues of dealing with the certification of information security management systems need to be considered and discussed thoroughly.

International Organization Standardization (ISO) had been supported by German Standardization Organization since 1983. It was separated from the Data Encryption Working Group of ISO No. 97 Technical Committee (TC) and became the twentieth single Sub-Committee (SC). It is formally called Data Cryptographic Techniques of ISO/TC97/SC20, and starts with the formulation of international standardization of information security technology. In 1989, ISO and International Electro Technical Commission (IEC) cooperate to set up the Information Technology (IT) Security Techniques (ST) of ISO/IECJTC/SC27. From 1990, ISO/IECJTC/SC27 began to set up international standardization of information security certification. On November 15, 1999, it proclaimed ISO/IEC 15408 as the paradigm of IT security assessment. It also announced ISO/IEC 17799 as the guidance of establishing information security management system on December first, 2000. The relevant standards that has been announced and worked on are listed in Table 4.1. ISO/IEC 19791 is the standard of operation environment security assessment, as shown in Fig. 3.4 [25–27]. In this paper, we proposed the information system security certification mechanism as indicated in Fig. 3.7, hoping to fulfill the aim of ISO/IEC 19791.

In the 1990s, the civilizations of the globe have undergone great changes, the quality, environment, and industry security sanitation management have been agreed upon and standardized. At the same time, national standardization has affected the economical development of many countries as well as the way of organization management. The obedience of ISO quality and environment management system standards is the best proof. The ISO standards related to information security have been successively an-

Table 4.2
Description of the ISMS Auditing Course

The course hoped that give lessons should be contains standards, law and regulations.	1. ISO/IEC TR 13335 (all parts) 2. ISO/IEC 21827 3. ISO/IEC 17799 (CNS 17799) 4. BS 7799-2: 2002 (CNS 17800) 5. ISO 19011 6. ISO/IEC 15408 (all parts) 7. ISO/IEC TR 15504 (all parts) 8. ISO 13491 (all parts) 9. Law related to information security (. . ., Electronic Signature Law, Communication Protection Supervision Law, Information Public Law et al.)
Minimal course time	56 h
Exercise assignments	1. Every day at least once. 2. One group contains five personnel. 3. A brief and discussion contains 60 min.
Testing	Every time 2 h, totally 4 h.
The amount of course	1. 12–20 (2 instructors) 2. 6–10 (1 instructor)

nounced, like ISO/IEC 15408, ISO/IEC 17799, and ISO/IEC 21827 (SSE-CMM). If they are properly applied, they will be helpful to the cultivation of digital security culture in Taiwan.

The security of information system is like a chain. Its strength is affected by the weakest knot. The description of ISMS auditing course mentioned here is based on Table 2.3 and Fig. 3.7, with the reference of Information Security Management System (ISMS) announced by the International Register of Certificated Auditor (IRCA) in Britain [24]. This description of ISMS auditing course in Table 4.2 is expected to perform the ISMS certification audit and be the basis of indispensable knowledge and skills required by ISMS auditing, as illustrated in Fig. 3.7.

The large use of commercial components to build the information system is inevitable. In integrating the old, new and future software, hardware, telecommunications, application systems, it is essential to know how to assure that the contracting firms can meet the security standards. Therefore, the audit personnel for the ISMS certification should be knowledgeable and skilled in CC, SSE-CMM and ISO/IEC 17799, etc. during performing the risk evaluation.

Acknowledgements

The authors would like to express our appreciation to the anonymous reviewers for their invaluable suggestions.

References

[1] M.-S. Cai, D.-Z. Wang, P.-H. Wang, Liberty Times (2003 May 28) 1 (Taipei).
[2] Y.-X. Chen, United Daily (2002 August 1) 8 (Taipei).
[3] X. Yan, Technology of Mainland China Hackers, Song-Gang Computer Publication Publishes, Taipei, Taiwan, 2000.
[4] H.-M. Lin and H.-Z. Qin, United Daily, July 21, 2002, p. 6, Taipei and Kaohsiung's City Online Report (2002).
[5] M. Swanson, Security self-assessment guide for information technology systems, NIST SP 800-26, NIST, 2001.
[6] NSA (National Security Agency), Information Assurance Technical Framework, Version 3.1, 2002, http://www.iatf.net.
[7] R. Ross, M. Swanson, Guide for the security certification and accreditation of federal information systems, NIST SP 800-37, NIST, pp. 1–62 (2003).
[8] NSTISSC (National Security Telecommunications and Information System Security Committee), National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSC, 2000.
[9] F.B. Schneider, et al., Trust in Cyberspace, National Academy Press, Washington, USA, 1999.
[10] ISO (International Organization for Standardization), Information technology—Security techniques—Evaluation criteria for IT security (All parts), ISO/IEC 15408: 1999(E), ISO, 1999.
[11] NIST (National Institute of Standards and Technology), Security requirements for cryptographic modules, FIPS PUB 140-2, NIST, 2001.
[12] S. Katzke, Protecting federal information systems and networks, Presentation of the 4th International Common Criteria Conference, Stockholm Sweden, 2003 Sept. 7–9.
[13] ISO/IEC JTC1/SC27, Information Technology—Security Techniques—A Framework for IT Security Assurance (All Parts), ISO/IEC 15443, ISO/IEC JTC1/SC27 N3592, N3605, and N3614, 2003.
[14] FAA (Federal Aviation Administration) FTI (Telecommunications Infrastructure) Program Documents, http://www.faa.gov/programs/fti/main.htm..
[15] ISO (International Organization for Standardization), Information technology—guidelines for the management of IT security—Part 1: concepts and models for IT security, ISO, 1996.
[16] NBS (National Bureau of Standards), Guideline for computer security certification and accreditation, FIPS (Federal Information Processing Standards), PUB (Publication) vol. 102, NBS, Gaithersburg, MD, USA, 1983.
[17] M.D. Abrams, P.J. Brusil, Application of the common criteria to a system: a real-world example, Computer Security Journal 16 (2) (2000) 11–21.
[18] D. Herman, S. Keith, Application of the common criteria to a system: a case study, Computer Security Journal 17 (2) (2001) 21–28.
[19] SSE-CMM (System Security Engineering Capability Maturity Model), Program Documents, http://www.sse-cmm.org.
[20] D.J. Out, How to write useful security targets, Presentation of the 4th Information Common Criteria Conference, Stockholm, Sweden, 2003 Sept. 7–9.
[21] K.-J. Farn, et al., A study on the certification of the information security management systems, Computer Standards and Interfaces 25 (5) (2003) 447–461.
[22] ISO/IEC JTC1/SC27, Information technology—Security techniques—Security assessment of operational systems, ISO/IEC 19791, ISO/IEC JTC1/SC27 N3596, 2003.
[23] R.J. Ellison, et al., Survivable network system analysis: a case study, IEEE Software 16 (4) (1999) 70–77.
[24] IRCA (International Register of Certificated Auditor), Program Documents, http://www.irca.org/auditortrain/auditor-train_2_1.html.
[25] M. Ohlin, Common criteria-related activities within International Standardization in JTC1/SC27, Presentation of the 4th Information Common Criteria Conference, Stockholm, Sweden, 2003 Sept. 7–9.
[26] S. Katzke, The common criteria (CC) Years (1993–2008):

looking back and ahead, Presentation of the 4th Information Common Criteria Conference, Stockholm, Sweden, 2003 Sept. 7–9.
[27] M. Ahlbin, P. Ronn, Implementation of an ISMS in the National Tax Board of Sweden, Presentation of the 4th Information Common Criteria Conference, Stockholm, Sweden, 2003 Sept. 7–9.

Kwo-Jean Farn is vice president of the R&D Department in Taiwan Internet Security Solutions and part-time associate professor of National Chiao Tung University (NCTU) in Taiwan. He received his PhD degree in 1982. During a 20-year career at Information Technology and 10-year career at Information Security. He is chair of the Implementation National Critical Information Infrastructure Protection Project at Computer and Communications Research Laboratories/Industrial Technology Research Institute (CCL/ITRI) in Taiwan from Jan. 1999 to Sep. 2000. He worked at ITRI for more than 18 years until summer of 2001. He have 9 patents of information security area.

Shu-Kuo Lin received his MBA degree in Information Management from Tam Kang University, Taiwan, in 2000. Currently, he is a PhD candidate of the Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan. His research interests include information security and network management.

Andrew Ren-Wei Fung received the BBA and MS degrees in Information Management form National Defense Management College, Taiwan, in 1987 and 1995, respectively. Currently, he is a PhD candidate in the Institute of Information Management, National Chiao Tung University (NCTU), Hsinchu, Taiwan. His research interests include information security and parallel computing.