Information Security Management Curriculum Design: A Joint Industry and Academic Effort

Ki-Yoon Kim
Department of Business Administration
Kwangwoon University
Seoul, Korea

Ken Surendran
Computer Science Department
Southeast Missouri State University
Cape Girardeau, MO 63701, U.S.A

ABSTRACT

In this paper the authors present a curriculum design for Information Security Management, which was synthesized using the inputs from both the industry and academia. The top down curriculum design process carried out in Korea starts with the analysis of the job of an Information Security Manager (ISM), identifies the knowledge elements needed for successfully fulfilling the main responsibilities of the job and finally synthesizes them into seven courses suitable for flexible implementation. Additionally, a lateral occupational analysis of ISM reveals the value-skills (soft-skills) that should be considered in the actual implementation of the curriculum.

Keywords: Information security management, curriculum development, Information Security Manager, job analysis.

1. INTRODUCTION

Information security is a discipline that is concerned with the implementation and support of security and control procedures to protect the availability, integrity and privacy of electronically stored data. In dealing with security, a *risk* is any hazard or danger to which a system or any of its components (e.g., hardware, software, information, or data) is subjected. *Threat* is any actor, action, or event that has a potential to be a risk in the above sense, and *vulnerability* is a point within a system that is susceptible to attack from a threat. With the rapid growth in the global Information Technology (IT) environment, increased levels of risks, threats and vulnerabilities are seen. Organizations have started employing Information Security Managers (ISM) to ensure availability, authenticity, confidentiality, integrity, and usability by protecting the information in all stages of input, process, and output (NIST 1990). As such, the ISM is responsible for an organization's information security policy and program support and for the selection and maintenance of specific safeguards/controls for the organization’s computer and communications network and application software. Sound curricula in Information Security Management are required to develop enough number of ISMs who can help ensure reliable deployment of IT.

In designing a curriculum for new or emerging occupational areas such as Information Security Management, a systematic approach like DACUM (Developing A CUrriculuM) lends itself conveniently to integrate the pragmatic perceptions of the practitioners in the industry and the rigorous prescriptions of the instructors in the academia. In adapting DACUM (Halasz 1994), material pertaining to ISM job can be gathered from best practitioners in that field to derive the job definition, job flow, and job description, and to develop the education/training programs with the help of instructors. Fundamentally, the DACUM process is brainstorming in a well-organized step-by-step manner. The method is based on the three premises that: (1) expert workers are better able to describe and define their occupation than anyone else; (2) any job can be effectively and sufficiently described in terms of tasks successful workers perform in that occupation; and (3) all tasks have direct implications for the knowledge and attitudes that workers must have in order to perform the tasks correctly. The DACUM forums on ISMs conducted in Korea had equal representation from both industry and academia. In this paper, the results of these DACUM forums leading to the design of a curriculum for Information Security Management are presented. In section 2, the main steps used in the curriculum design process are described. In section 3, the results of ISM job analysis are presented. A comprehensive education/training program for developing qualified ISMs is derived in section 4. In this, using a lateral occupational analysis, the value-skills of ISM are identified for use in the actual curriculum implementation.

2. CURRICULUM DEVELOPMENT METHODOLOGY

The main process consists of gathering and recording valid information about a specific job and about the skills desired in a person, who performs that job. This includes: the activities and responsibilities, which make up the job; the skills, knowledge and abilities needed by its incumbent for effective performance; and the standards or targets, which provide the basis for assessing performance. The key objective in job analysis is to identify the *tasks* to be carried out by an ISM. *(* A *task* is a major job activity that consists of one or more *work(s)* and leads to a product, service, or decision. Each *work* is a specific step in fulfilling the *task*.) Job analysis is a process where judgments are made about data collected on a job. The analysis helps in identifying the major *tasks* that are specific to the job and the *works* that are carried out in the identified *tasks*.

The entire procedure used for designing the Information Security Management curriculum consisted of five steps as summarized in Table-1. Step 1 was the preparation for job analysis. The job analyst identified ISM as a new occupation in Korea and, in order to come up with a suitable education and training program, organized a DACUM committee, consisting of five Subject Matter Experts (SMEs) and five instructors. The ten panel members first attended an intensive 3-day workshop on DACUM concepts, which was facilitated by a specialist from KRIVET (Korea Research Institute of Vocational Education and Training). Five high performers in the field of information security from different organizations were chosen as SMEs. The instructors were professors from the Korea Institute of Information Security and Cryptology (KIISC). With the guidance of a DACUM facilitator, the process began by choosing a job title (in this case already identified as ISM) and job definition. The panel then identified the *tasks* of ISM.

Table 1: Procedure of Job Analysis

Steps	Procedure	Methods	Results
Step 1	Preparation for job analysis	Data collection and interviews	Collection of related information and data. Organizing of DACUM committee.
Step 2	Job/task analysis	DACUM	Flowchart of task and work. Job description including definition of occupation and job.
Step 3	Work analysis	DACUM	Work analysis including skills, knowledge, and tools for work.
Step 4	Education /training program develop-ment	DACUM	Key works/education contents matrix, Key works/courses matrix. Course profile and education/ training road map.
Step 5	Validation	Interviews	Modification and documentation of results

In step 2, task analysis was carried out. The instructors made a task-work flowchart and carried out the basic capability analysis for the ISM occupation. In addition, in this step, a job profile was created, which consisted of a job description and a listing of knowledge, skills, and traits needed by high performers in ISM. The DACUM committee also identified the most critical and frequently performed tasks and works, as well as those in which new and veteran workers were most in need of training or technical assistance. Step 3 dealt with work analysis. The instructors measured the difficulties of *work elements* (which are the subset of *work*), and identified the related skills, knowledge, and tools for each of the *works* of ISM.

In step 4, the education/training program was designed collaboratively. First, the instructors came up with a draft list of education elements in security area. The panelists were asked to evaluate the results generated till then and review the education elements list.

By mapping the education contents for the key works the forum constructed a key works/education contents matrix and also a key works/courses matrix. In all, seven courses constituted the core of the curriculum. Using these matrices, the instructors developed the course profile and the education/training roadmap. Step 5 was the validation process to ensure that the curriculum design met the needs of the employers and the expectations of the faculty. The validation process of an education/training program requires the involvement of industry as well as the instructional expertise of the faculty. Therefore, the committee members compared the program’s learning outcomes to the industry requirements, revising the learning outcomes as required. The draft job analysis and curriculum design were then reviewed and edited, and partly modified through field-interviews.

3. RESULTS OF ANALYSIS

The results of job analysis on ISM are presented in this section. The tasks and the associated works are listed in Table-2. In the following section, these tasks and works are described, a formal job description is given, and the required training associated with each task is identified.

3.1 Job of ISM

The job analysis indicated that the ISM's functions are planning, organizing, directing and implementing, reporting and communicating, and supporting incident response or investigation to successfully implement and manage the information security program (BSI 1999; ISO 1996). First, The ISM is responsible for planning all aspects of the information security program including the process for establishing or updating policies and standards encompassing security requirements as applicable. Second, the ISM identifies the resources needed to maintain the effectiveness of the program and works with senior management to assign responsibilities throughout the organization. Third, the ISM directs the activities of the information security function and monitors the organization's compliance with the information security program. Fourth, the ISM promotes information security awareness throughout the organization to all levels of management and to all employees and professional staff members. In particular they must be made aware of the need to report to the ISM all breaches of confidentiality and violations or suspected violations of security policy.

The identified tasks (see Table-2) are titled Security Policy, Risk Management, Safeguard Implementation, and Safeguard Maintenance Management. First, Security Policy describes the ideal status toward which all-organizational security efforts should lead. Security Policy requires knowledge of threats to systems, areas exposed to those threats, and the countermeasures that can be instituted (ISO 1997). The two works in Security Policy are *analysis of security requirements* and *documentation of security policy*.

In the second task, risks to critical and sensitive administrative information resources must be managed. Such risks may relate to the physical security of computer and communications networks, to the integrity of data maintained or transmitted within those systems, as well as to the stability and reliability of the associated application. The five works in Risk Management are *risk analysis*, *selection of safeguards, test of selected safeguard, development of security guidelines,* and *security aggregate planning*. Risk analysis is the basis for Risk Management; i.e., assumption of risks and potential losses, or selection and implementation of cost effective controls and safeguards to reduce risks to an acceptable level (ISO 1998). Absolute security that assures protection against all potential threats is unachievable; therefore, a means of weighing possible loses which could occur against the cost of mitigating controls is required. This weighing of potential risks verses control costs involves use of a systematic risk analysis methodology for evaluating vulnerabilities and threats to information resources. The selection and test of security safeguards are carried out in such a way to assure program compliance and the ongoing viability and integrity of organizational IT resources. Following this, appropriate security guidelines are prepared and the comprehensive safeguard architecture is documented in the security aggregate plan (ISO 1999).

Third, Safeguard Implementation should take into consideration the purpose for which the safeguard is intended and the environment in which the safeguards will be operating. Safeguards are often designed to serve one of the following functions – prevention, deterrence, containment, detection, and recovery. The implementation will be incomplete without training the employees in the organization.

Fourth, Safeguard Management ensures the successful operation of the implemented safeguard and the realization of the anticipated level of protection.

Security is more than keeping hackers and other troublemakers out of the system. It involves a host of internal practices that serve to protect information in the case of system or hardware failure. A complete security audit should include an examination of policies that affect or are affected by system security, as well as a thorough test of each mechanism that is in place to enforce said policies. Response to the security incidents should be swift and proactive where possible to prevent further damage. Some of the main activities security managers engage in on a day-to-day basis include administering backup and virus protection mechanisms, staying abreast of software updates, managing user accounts, and monitoring system activity (ISO 2000).

Table 2: Tasks and Works of ISM

- A. Security policy
  - A-1. Analysis of security requirements
  - A-2. Documentation of security policy
- B. Risk management
  - B-1 Risk analysis
  - B-2 Selection of safeguard
  - B-3 Test of selected safeguard
  - B-4. Development of security guideline
  - B-5. Security aggregate planning
- C. Safeguard implementation and training
  - C-1. Safeguard implementation
  - C-2. Education and training
- D. Safeguard management
  - D-1. Operation and maintenance
  - D-2. Security audit and review
  - D-3. Emergency response to security incidents
  - D-4. Monitoring

3.2 Job Description of ISM and Training

The job description for the ISM is presented here. The panel focused on the works, identified in step 2, and derived a job description for ISM (see Table 3), listing the four tasks and thirteen works, and rating the main characteristics for each work. They then considered the *difficulty* of the work (in terms of learning it), the *importance* of the work (in performing it correctly), and the f*requency* of the work (performed) as characteristics for describing the works. Here, each work was rated (based on their personal experience and in relation to other works) for each of these three characteristics on a 5-point scale from least to greatest (for instance, *difficulty* is rated in the ascending order: very easy, easy, average, hard, very hard).

The need for education for carrying out the works was rated on a 3-point scale: critical, important, and supportive (see Table 4). After examining the results in Tables 3 and Table 4, the panel decided that works with ratings *difficulty* and *importance* are more significant and crucial in further analysis. Works in the critical and important categories are considered key works for the job from education point of view. It was observed that every work except *development of security guideline* is a key work. The most suitable method for implementing the education/training for each of the 12 key works was identified from the four possibilities: CT (Classroom Training), JA (Job Aids), OJT (On-the-Job Training), and RT (Re-Training). The *difficulty* (in terms of learning the work) characteristic was determined to have the greatest influence on curriculum development. The next step was to describe each key work in detail from the perspective of just the *difficulty* characteristic. As an illustration, the description for *risk analysis work* is discussed here with its results summarized in Table 5 for the *difficulty* characteristic. Risk analysis is the process of identifying risks, determining their relevant magnitude and identifying appropriate safeguards. In detail, risk analysis is the process of identifying: (1) strategies of risk analysis, (2) all assets an organization possesses, (3) all potential threats to those assets, (4) all points of vulnerability to those threats, (5) the probability of potential threats being realized, the cost estimates of potential losses, and (6) documentation of a checklist for vulnerability evaluation. All the 13 work description tables are available in the DACUM report (Tables A1 – D4 in Na 1999).

Knowledge, skill, materials and equipment (items 4-6 in Table 5) are required to perform the job. Job analysis typically only states the minimum requirements to perform the job. Panelists are asked to identify the areas of knowledge that a successful ISM should posses. The DACUM committee after considering the skills that are necessary to perform the job came up with the following list: accounting, finance, statistics, network, operating system, information system, hacking, virus in the knowledge category. In addition, there are tools for risk analysis and business impact analysis, and skills to use those tools and document results of risk analysis. Some tasks and works are performed using information and equipment. Information for risk analysis work include asset list, threats statistics, vulnerability evaluation checklist; equipment for risk analysis includes a server, PC, printer, risk analysis software. This is just an illustration for dealing with one characteristics of a single work. The descriptions for the remaining 35 work-characteristics combinations can be found in the ISM DACUM committee report (Na 1999).

4. CURRICULUM DESIGN

While there may be several education/training courses available on information security management, there is currently no clear and systematic path for identifying the kind of education/training that will result in the required learning in relation to ISM's job or its key works requirements. Additionally, the technology changes rapidly, resulting in the need for regular updating of education contents. Consequently, course contents have to be constantly changed. Thus, any systematic effort to train ISMs must account for changing technical requirements and education contents (Laswell 1999). In order to develop a flexible curriculum that takes into account the above practical concerns, the relationships between the key works and education contents are established and the abstraction of education contents mapped into courses.

4.1 Key Works/Education Contents Matrix and Key Works/Courses Matrix

The purpose of training is to teach people the skills that will enable them to perform their jobs more effectively, and education is more in-depth than training, as it is targeted for professionals whose jobs require expertise in IT security. The training is required for individuals whose role in the organization indicates a need for special knowledge of IT security threats, vulnerabilities, and safeguards. The training program of the learning continuum strives to produce relevant and needed security skills and competency by practitioners of functional specialties other than IT security. The education program integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multi-disciplinary study of concepts, issues, and principles. Additionally, the program strives to produce IT security specialists and professionals capable of vision and pro-active response (Wilson 1998). Using the results of the job analysis carried out for ISM, a matrix for key works and education contents is first prepared (see Table 6) The purpose of such a matrix is to infer the necessary knowledge, functions, and tools for implementing the key works. The two key works *selection of safeguards* and *test of selected safeguards* are found to be related with most of the identified education contents From the perspective of education contents, *information security law (item 1) and standards* and *e-commerce security* (item 13) are deeply related with most of the key works.

Table 3: Job description and work list

Task	Name of work	Difficulty	Importance	Frequency
A. Security policy	Analysis of security requirements Documentation of security policy	①②③④❺ ①②③④❺	①②③④❺ ①②③④❺	①❷③④⑤ ❶②③④⑤
B. Risk management	Risk analysis Selection of safeguard Test of selected safeguard Development of security guideline Security aggregate planning	①②③④❺ ①②③❹⑤ ①②③❹⑤ ①❷③④⑤ ①②❸④⑤	①②③❹⑤ ①②③❹⑤ ①②③❹⑤ ①②❸④⑤ ①②③④❺	❶②③④⑤ ①②❸④⑤ ①②❸④⑤ ①②③❹⑤ ①❷③④⑤
C. Safeguard implement & train	Safeguard implementation Education and training	①②❸④⑤ ①❷③④⑤	①②③❹⑤ ①②③④❺	①②③❹⑤ ①②③④❺
D. Safeguard management	Operations and Maintenance Security audit and Review Emergency response to security incidents Monitoring	①②❸④⑤ ①②❸④⑤ ①②③④❺ ①❷③④⑤	①②③④❺ ①②③❹⑤ ①②③④❺ ①②③❹⑤	①②③④❺ ①②❸④⑤ ❶②③④⑤ ①②❸④⑤

Table 4: Rating of educational needs for works

Key Task									
Task	No	Name of work	Education necessity			Education methods			
			CRI	IMP	SUP	CT	JA	OJT	RT
A. Security policy	1	Analysis of security requirements		●		●			
	2	Documentation of security policy		●		●		●	
B. Risk management	1	Risk analysis		●		●	●	●	
	2	Selection of safeguard	●			●		●	
	3	Test of selected safeguard	●			●		●	
	4	Development of security guideline			●			●	
	5	Security aggregate planning		●				●	
C. Safeguard implementation & training	1	Safeguard implementation	●			●	●	●	●
	2	Education and training		●		●		●	
D. Safeguard management	1	Operations & maintenance	●				●	●	●
	2	Security audit & review		●		●		●	
	3	Emergency response to security incidents		●		●		●	●
	4	Monitoring		●		●		●	

Table 5: Work description of risk analysis

1. Name of Work	B-1 Risk analysis	
2. Achievement Level	It is possible to evaluate vulnerability of information assets against threats by risk analysis.	
3. Work Elements		Difficulty
(1)	Choice of risk analysis strategy	①②③❹⑤
(2)	Asset analysis that classified, identified, evaluated property of information assets	①②③④❺
(3)	Threat analysis that classified, identified, measured the threat or event behaviors	①②③④❺
(4)	Vulnerability evaluation that identified disadvantages of information system damaged by the source of threats	①②③④❺
(5)	Business impact analysis for nature hazards or human disaster	①②③④❺
(6)	Documentation of checklist for vulnerability evaluation	①②③❹⑤
Difficulty average		①②③④❺
4. Related Knowledge & Skill		
Knowledge	Skill	
Accounting and finance, statistics, network, operating system, information system, hacking, and virus.	Risk analysis tool, business impact analysis, documentation	
5. Requirements Materials	Asset list, threats statistics, vulnerability evaluation checklist	
6. Requirements Equipments and Tools	Server, PC, printer, risk analysis s/w	

The goal of the *key work/course* matrix (Table 7) is to classify necessary knowledge, functions, and tools according to their degree of influence on the key works, and use this information for deducing the necessary courses for each key

The logically identified education and training courses are: System Security (I, II), Network Security (I, II) and Application Security (I, II), and Information Technology Risk Management. The System Security course segment considers potential threats and vulnerabilities that are directly related to a system's information. It assessing the risk to automated information resources and information and determining adequacy of safeguards. The main outcomes consist of analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk. As shown in Table 7 documentation of security policy, risk analysis, and security aggregate planning are mainly related with IT Risk Management. A few key works - analysis of security requirements, selection of safeguard, and test of selected safeguard - have learning components in all courses.

4.2. Value Skills

It is useful to identify the value skills (soft-skills) of ISM as they can be used in the actual implementation of the curriculum. An ISM plays several roles, which involve professional relationships, in carrying out the job. Such role-plays provide opportunities to apply and develop various value skills (Surendran, 2002). In examining the ISM as an occupation, the DACUM panel identified the ISM's interactions with related occupations and the abilities for the ISM. In describing these aptitudes, the panel suggested the ISM should have leadership for responding to security accidents and should exercise patience while managing safeguards. Intrinsic to these basic abilities are the following value skills: Communication (including information handling and proficiency in foreign language), Business-sense (organization values, priorities), Inter-personal (co-operative attitude, delegation, leadership, conflict management), Personal-development (plan and execute self-development, value system, attitude about occupation). When implementing the actual curriculum these factors should be taken into account – either in individual courses or by incorporating into the curriculum an internship where opportunities to develop such value skills exist.

4.3 Course Profile and Education Training Road Map

The panel prepared profiles for the seven courses identified earlier on. The course profile is the starting point for the development of a suitable course description and the design of the course itself. Course profiles are included in the DACUM report (Na 1999). These course profiles were later validated with the industry for their correctness and with the educational institutions for the feasibility and completeness of the focuses on maintaining information confidentiality, integrity, and availability, and recommends strategies for protecting information while in transmission (manual and local), in use, and in storage. The Network Security (including the Internet) recommends strategies for protecting the network when connecting to other networks, and for transmitting information over the Internet in a secure manner. The Application Security focuses on potential threats to computer software and specific countermeasures to those threats and software-related vulnerabilities. The Information Technology Risk Management deals with the ongoing process of program. Specifically, checks are made to ensure that the learning outcomes do indeed realize the industry requirements.

The panel suggested an education/ training roadmap for offering the seven courses identified for the ISM curriculum. As shown in Figure 1, the three basic courses may be offered at the 2-year college level (termed as the 3rd occupation competence in Korea) and the remaining four courses offered at 4-year university level (termed 4th occupation competence in Korea).

5. CONCLUSION

The curriculum development process is based on an objective, analytical technique that has been found to be quick, effective and inexpensive. The results included the job definition, job flowchart, job description, and the curriculum for ISM. An education/training roadmap was also suggested, indicating the levels at which the courses could be offered. Following this study, the academic institutions are continuing to make detailed course descriptions. This study was conducted in Korea as a collaborative effort between industry and academia in 1999. Since then a study in Korea (Kim 2001) indicates that some Information Security Management curricula use 15 key-courses that include Introduction to Information Security, Communication Ethics, Information Theory and Computation Theory, Algebra, Steganography. Another recent contribution (Kim 2002) identified 15 most significant educational requirements for different categories of professionals in the Information Security field. The additional element identified in this study is Ethics. However, the design of the seven courses is flexible enough to incorporate such additional requirements.

As part of the study, the DACUM panel also designed a draft occupation description for possible adoption in Korea. The occupation description provides a practical perspective for the ISM job.. In this description, the requirements for value skills such as *communication* and *interpersonal* are identified.

The job analysis process has several limitations including: (a) items and rating scales that are so behaviorally abstract that it is difficult to collect accurate

Table 6: Key works/education contents matrix

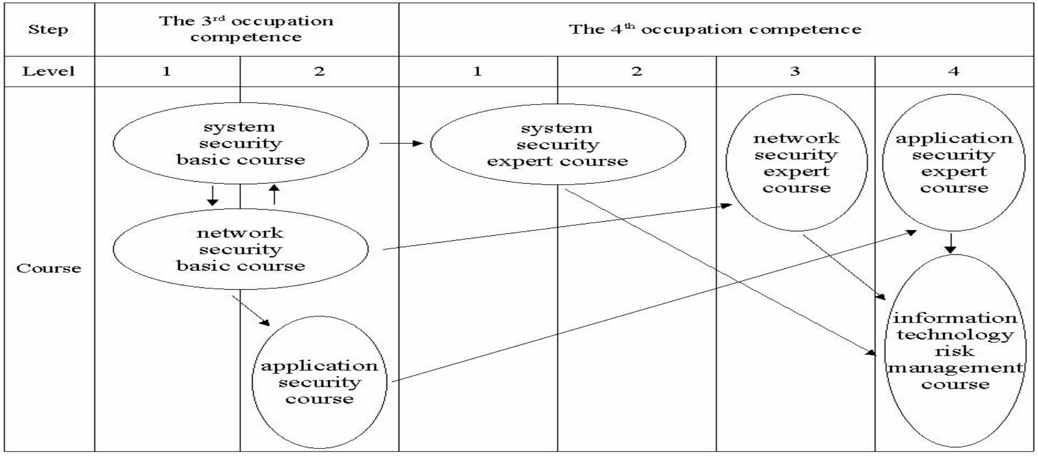
Key Works↓ Education Contents*→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Analysis of security requirements	●	●											●					
Documentations of security policy	●												●					
Risk analysis	●									●	●	●	●	●	●	●	●	
Selection of safeguards	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●
Test of selected safeguard	●		●	●	●	●	●	●	●	●		●	●	●			●	●
Security aggregate planning	●	●												●		●	●	
Safeguard Implementation	●		●	●	●	●	●	●	●	●		●						●
Education and training	●				●	●					●	●	●					
Operation & maintenance		●	●	●	●	●	●	●	●	●		●	●					
Security audit & review	●												●		●			
Emergency response to incidents	●										●		●					
Monitoring			●	●	●	●	●	●	●	●		●	●		●			

* 1: Info security law and standards, 2: Info-system analysis design, 3: System security technology, 4: Database, 5: Operating system, 6: Network security, 7: Intrusion detection and interception, 8: Network, 9: Network security tech., 10: Virus, 11: Hacking case, 12: Web security, 13: E-commerce security, 14: Accounting and finance, 15: Statistics, 16: Risk analysis, 17: Decision theory, 18: Cryptology

Table 7: Key works/course matrix

Courses Key Works	1	2	3	4	5	6	7
	System security –I	System security -II	Network security –I	Network security -II	Application security -I	Application security -II	Information technology risk management
A-1 Analysis of security requirements	●	●	●	●	●	●	●
A-2 Documentation of security policy							●
B-1 Risk analysis							●
B-2 Selection of safeguard	●	●	●	●	●	●	●
B-3 Test of selected safeguard	●	●	●	●	●	●	●
B-5 Security strategy and planning							●
C-1 Safeguard implementation	●	●	●	●	●	●	
C-2 Education and training	●	●	●	●	●	●	
D-1 Maintenance	●	●	●	●	●	●	
D-2 Security audit	●	●	●	●	●	●	
D-3 Response to security incidents	●	●	●	●	●	●	
D-4 Monitoring	●	●	●	●	●	●	

Figure 1: Education/training roadmap


Step
The 3rd occupation competence
The 4th occupation competence
Level
1
2
1
2
3
4
Course
system security basic course
network security basic course
application security course
system security expert course
network security expert course
application security expert course
information technology risk management course

and verifiable data (Harvey 1991); and (b) deficiencies in content coverage, especially for success

The outcomes of such job analysis depend heavily on the panel. Some other committee with a different set of membership could come up with a different curriculum prescription for ISM. The process relies on two critical factors for its The first is selecting the right panel. Some supervisors may intimidate their employees (if they are also present in that group). This may result in non-participation in the development process. Also, some instructors in the panel may tend to push the panel toward their own training programs. The second criterion is having a skilled facilitator. The facilitator must guide the panel through the process without prejudice and must ensure that the panel comes to consensus on every item on the agenda.

The present study makes several contributions to both the adoption of the job analysis method and to education /training program development for ISM as a new occupation in Korea. The primary methodological contribution was the combination of job analysis and interviews, including the final validation step in which the committee reviewed the feedback from industry and academia. This technique can be applied to other educational programs as well, in order to fine-tune them by using the validation step.

Even though this study was carried out in Korea, its results can be applied in other countries, with suitable changes to accommodate the differences in the IT security environment in comparison to Korea. In countries, which do not have a specific Information Security Management curriculum, there probably exist several curricula in Computing and in IS which generally offer three streams, specializing in areas like application development, communications network, and database management. The authors recommend that the first three basic courses (system security, network security and application security) identified in this study be offered as optional courses in the existing curricula in order to increase the security awareness.

5. ACKNOWLEDGEMENTS

This study was supported by Kwangwoon University during Ki-Yoon Kim's sabbatical year 2001 at UNITEC Institute of Technology, Auckland, New Zealand, where Ken Surendran was a faculty member till July 2001. The authors wish to thank Dr Helen Hays (SEMO-SU) for her suggestions in improving the quality of this publication.

6. REFERENCES

BSI (British Standards Institute) [1999], *Information Security Management – Part 1: Code of Practice for Information Security Management*, BSI 7799-1. http://www.bsi-lobal.com/Information+Security+Homepage

Halasz, Ida M., [1994], *Overview of the DACUM Job Analysis Process*, Report 199-I, US Department of Justice National Institute of Corrections, NIC Academy, September, 1-3.

Harvey, Robert. J., [1991], Job Analysis, *Handbook of Industrial and Organizational Psychology*, M. D. Dunnette and L. M. Hough (Eds.), Palo Alto, CA: Consulting Psychologists Press.

ISO, [1996-1999],. Guidelines for the Management of IT System Security: Part 1-5, ISO/IEC JTC1/SC27 TR 13335

Kim, Cheul, [2001], "Development of Information Security Education Course in the Universities," *KIISC (Korea Institute of Information Security & Cryptology) Review*, Vol.11, No. 3, pp. 75-89

Kim, Sehun. and Myeong-Gil Choi, [2002],"Education Requirement Analysis for Information Security Human Resources in Korea," Working Paper, KAIST, pp.1-23.

Laswell, Barbara. S., Derek. Simmel, and Sandra. G.Behrens, [1999], *Information Assurance Curriculum and Certification: State of Practice*, Technical Report, Software Engineering Institute, Carnegie Mellon University.

Na, Hyun-Mi, Ki-Yoon Kim, Zon-Sik Kang, Jung-Duck Kim, Young-Su Sin, Jong-Cheul Sim, Sung-Keun Lee, Ki-Ju Youn, Jong-Lack Choi, Jong-Uk Choi, and Heu-Sun Hwang, [1999], *Job Analysis for Information Security Manager*, Report 99-9-8, Korea Research Institute of Vocational Education and Training.

NIST, [1990], *Simplified Risk Analysis Guidelines*, NISTIR 4387, U.S. Department of Justice.

Surendran, Ken, Helen Hays, and Andrew Macfarlane, [2002],"Simulating a Software Engineering Apprenticeship", IEEE Software (to appear in September / October issue).

Wilson, Mark., Dorothea. E. de Zafra, Sadie. I. Pitcher, John. D. Tressler, and, John. B. Ippolito., [1998], *Information Technology Security Training Requirements: A Role- and Performance- Based Model,* National Institute of Standards and Technology, U.S. Department of Commerce, 16.

AUTHOR BIOGRAPHIES

Ki-Yoon Kim is a Professor in and the Chairman of the Department of Business Administration at Kwangwoon University, Seoul, Korea. . His research focuses on Security Management, Software and Information System Risk Management. He received his Ph.D. in Management Science at the Korea University in Korea

Ken Surendran is an Associate Professor in the Department of Computer Science at Southeast Missouri State University. His research interests include Software Engineering and Security Management Education. His industrial experiences in IT were with Indian Space Research Organization and Zambia Consolidated Copper Mines. His previous academic assignments in IT were with Rose-Hulman Institute of Technology; UNITEC Institute of Technology, New Zealand; Copper-belt University, Zambia; and PSG College of Technology, India. Surendran received a B.E. in Electrical Engineering from University of Madras, India, M. Tech. in Electrical Engineering from Indian Institute of Technology, Madras, India, and Ph. D. in Applied Analysis from State University of New York at Stony Brook. He is a senior member of IEEE and a member of ACM.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096