

A Curriculum Development For Information Security Manager Using DACUM

Ki-Yoon Kim¹

Department of Business Administration, Kwangwoon University
Seoul, Korea

and

Ken Surendran²

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

Abstract

Generally, the Information Security Manager (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. In this paper, the authors present, based on a systematic job analysis, the definition, flowchart and description of ISM's job for developing an ISM education and training program for consideration in Korea. The result of this study reveals that there are 4 *tasks* and 13 *works* in the job of Information Security Manager, and 18 education contents and 7 education courses in the ISM curriculum.

Keywords: Information security manager, curriculum development, DACUM, job analysis

1. INTRODUCTION

Information technology is the central nervous system of today's organizations, exchanging information that is vital to their survival. Rapid changes in our technical environment, resulting in potential vulnerability of major information systems, have caused increased concern about the selection, deployment and maintenance of adequate security controls. 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. Information security is that discipline concerned with the implementation and support of security and control procedures to protect the privacy, integrity and availability of electronically stored information.

It is the job of an Information Security Manager (ISM) to ensure confidentiality, integrity, availability, authenticity, and usability by protecting the information in all stages of input, process, and output (NIST 1990).

A sound education program, designed through formal job analysis, helps develop qualified ISMs. DACUM (Developing A Curriculum) is a job analysis method used to create descriptions for new or emerging occupational areas and new education/training programs (Halasz 1994). In DACUM, material pertaining to a job is gathered from best practitioners in that field to derive the job definition, job flow, and job description, and to develop the education/training programs.

In this paper, the DACUM method is applied to analyze and describe the ISM job. In section 2, the procedure used for analyzing the ISM job is described. In section 3, the results of ISM job analysis are presented, using material gathered from DACUM forums conducted in Korea. In section 4, a comprehensive education/training program for developing qualified ISMs is suggested.

2. JOB ANALYSIS 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

¹ min1203@daisy.kwangwoon.ac.kr

² ksurendran@semovm.semo.edu

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 basic unit of a job is the performance of specific *duties* and *tasks*. *Duty* is a general area of competence that successful professional in an occupation must demonstrate or perform on an on-going basis. A duty includes one or more distinct *tasks*. 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 developing a statement of *duties*, and in identifying the major *tasks* that are specific to the job and the *works* that are carried out in the identified tasks. The purpose of job analysis is to establish and document the different dimensions of the job, such as education, training, selection, compensation, and performance appraisal.

2.1 DACUM - a Job Analysis Method

DACUM is a quick, yet highly valid job analysis technique. The DACUM process is used to determine the competencies that should be addressed in an education/training program for a specific occupation. This cost-effective and efficient technique has been validated through research and compares very positively with other job analysis methods (Halasz 1994). It is also an approach to occupational analysis in terms of tasks, works, knowledge, skills, traits and attitudes discussed earlier. The DACUM 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. (3) All tasks have direct implications for the knowledge and attitudes that workers must have in order to perform the tasks correctly.

Fundamentally, the DACUM process is brainstorming in a well-organized step-by-step manner. The process requires a panel of 5 to 10 experts in the occupation being analyzed, a qualified DACUM facilitator, and a recorder. The facilitator must be able to elicit specific task statements, deal with conflict and debate when the panel is reaching consensus, and continually forge ahead in order to complete the process. The experts participate in informative DACUM workshops where they learn a great deal about their jobs and how others view their work. During the DACUM work session, the facilitator systematically guides the panel members through brainstorming and consensus-reaching discussions to describe their job in terms of main duties and specific tasks. The panel members also agree on the relevant attitudes, knowledge, and skills as well as the primary tools of their job. The recorder writes the duties and tasks on large index cards that are taped or pinned to a wall facing the panel. This storyboarding process is essential to successful DACUM profiles because the cards are replaced, reworded, and rearranged until the

panel members agree that it is an accurate profile of their job. The DACUM analysis uses focus groups of workers who are high performers in the occupation to describe the duties and tasks, which are included in the given occupation. The DACUM process yields an occupational profile.

2.2 DACUM Process for ISM

The entire DACUM process used for ISM 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 5 Subject Matter Experts (SMEs) and 5 instructors. The ten panel members first attended an intensive 3-day workshop on DACUM process, 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 Korea Institute of Information Security and Cryptology (KIISC). With the guidance of a DACUM facilitator, the DACUM process began by choosing a job title (in this case already identified as ISM) and job definition. The panel then identified duties and the job tasks.

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 developed. The panelists were asked to evaluate the results of the DACUM process and were issued with a draft education/training program. After analyzing key works/education contents matrix and key works/courses matrix, the Instructors developed the course profile and the education/training roadmap.

Step 5 was the validation process. Finally, program validation was used to ensure that it 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 then compared the program's

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 development	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

Table 1. Procedure of job analysis

learning outcomes to the industry requirements, revising the learning outcomes as required. The draft job analysis and program were then reviewed and edited, and partly modified through field-interviews.

3. RESULTS OF JOB ANALYSIS ON ISM

The results of job analysis on ISM are presented in this section. It describes the 4 tasks and 13 works, which were identified as central to the job of ISM by the DACUM panel in Korea. The tasks and the associated works are listed below. These are extracted from the flow chart for task-work.

- 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
 - D-4. Monitoring

In the following section, these tasks and works are described, a formal job description is given, and the required training for each task is identified.

3.1 Job of ISM

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 are titled Security Policy, Risk Management, Safeguard Choice, 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*.

Second, 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 losses 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 disk 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).

3.2 Job Description of ISM and Training

The job description for the ISM is presented here. The DACUM panel focused on the works, identified in step 2, and derived a job description for ISM (see Table 2), listing the 4 tasks and 13 works, and rating the main characteristics for each work. The DACUM committee considered the *difficulty* of the work (in terms of learning it), the *importance* of the work (in performing it correctly), and the *frequency* of the work (performed) as characteristics for describing the works. Here, each work was rated (based on their 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 is measured on a 3-point scale: critical, important, and supportive (see Table 3). After examining the results, the panel decided that *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. Therefore, 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 is, therefore, 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 4 for the *difficulty* characteristics. 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 Kim 1999).

Knowledge, skill, materials and equipment 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 possess. 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.

The above is just an illustration for dealing with one characteristic of a single work. The descriptions for the remaining 35 work-characteristics combinations can be found in the ISM DACUM committee report (Kim 1999).

4. CURRICULUM DEVELOPMENT FOR ISM

While there may be several education/training courses available on information security management, but 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

Task	Name of work	Difficulty	Importance	Frequency
A. Security policy	Analysis of security requirements	①②③④⑤	①②③④⑤	①②③④⑤
	Documentation of security policy	①②③④⑤	①②③④⑤	①②③④⑤
B. Risk management	Risk analysis	①②③④⑤	①②③④⑤	①②③④⑤
	Selection of safeguard	①②③④⑤	①②③④⑤	①②③④⑤
	Test of selected safeguard	①②③④⑤	①②③④⑤	①②③④⑤
	Development of security guideline	①②③④⑤	①②③④⑤	①②③④⑤
	Security aggregate planning	①②③④⑤	①②③④⑤	①②③④⑤
C. Safeguard implement & train	Safeguard implementation	①②③④⑤	①②③④⑤	①②③④⑤
	Education and training	①②③④⑤	①②③④⑤	①②③④⑤
D. Safeguard management	Operations and Maintenance	①②③④⑤	①②③④⑤	①②③④⑤
	Security audit and Review	①②③④⑤	①②③④⑤	①②③④⑤
	Emergency response to security incidents	①②③④⑤	①②③④⑤	①②③④⑤
	Monitoring	①②③④⑤	①②③④⑤	①②③④⑤

Table 2. Job description and work list

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 3. Key task of job description

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	①②③④⑤
(2)	Asset analysis that classified, identified, evaluated property of information assets	①②③④⑤
(3)	Threat analysis that classified, identified, measured the threat or event behaviors	①②③④⑤
(4)	Vulnerability evaluation that identified disadvantages of information system damaged by the source of threats	①②③④⑤
(5)	Business impact analysis for nature hazards or human disaster	①②③④⑤
(6)	Documentation of checklist for vulnerability evaluation	①②③④⑤
Difficulty average		①②③④⑤
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	

Table 4. Work description of risk analysis

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 5). 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 related with most of the identified education contents. From the perspective of education contents, *information security law and standards* and *e-commerce security* are deeply related with most of the key works.

The goal of the *key work/course* matrix (table 6) 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 work. The logically identified education/training courses for the ISM are: System Security (I, II), Network security (I, II), Application Security (I, II), and Information Technology Risk Management.

System Security considers potential threats and vulnerabilities that are directly related to a system's information. It 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 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 6 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 Course Profile and Education Training Road Map

The next step is to prepare profiles for each of the identified courses. 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 (Kim 1999).

The DACUM committee 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 are offered at 4-year university level (termed 4th occupation competence in Korea).

These course profiles were later validated with the industry for their correctness and with the educational institutions for the feasibility and completeness of the program. Specifically, checks are made to ensure that the learning outcomes do indeed realize the industry requirements.

5. CONCLUSION

An ISM's job is to manage confidentiality, integrity, availability, authenticity, usability of information and service provided in the information system. The current level of information security breaches reported and the potential impacts they carry indicates that there will soon be a very high demand for qualified ISMs with formal training.

This study was conducted in Korea using the DACUM approach, which is an objective, analytical technique that has been found to be a quick, effective and inexpensive methodology for job analysis. 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 these seven courses could be offered. Following this study, the academic institutions are presently making detailed course descriptions.

As part of the study, the DACUM panel also designed

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 5. Key works/education contents matrix

Key Works \ Courses	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 aggregate planning							●
C-1 Safeguard implementation	●	●	●	●	●	●	
C-2 Education and training	●	●	●	●	●	●	
D-1 Maintenance	●	●	●	●	●	●	
D-2 Security audit	●	●	●	●	●	●	
D-3 Response of security incidents	●	●	●	●	●	●	
D-4 Monitoring	●	●	●	●	●	●	

Table 6. Key works/course matrix

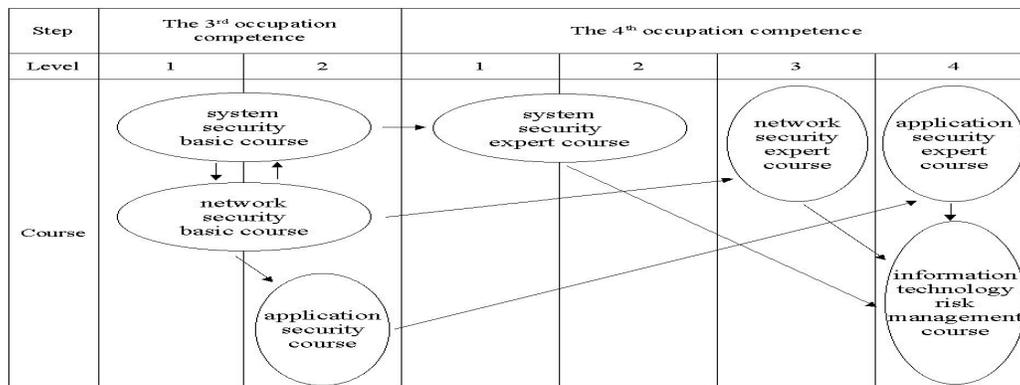


Figure 1. Education/training roadmap

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 supporting skills such as *communication* and *interpersonal* are identified.

The worker-oriented instruments for job analysis have several limitations including: (a) items and rating scales that are so behaviorally abstract that it is difficult to collect accurate and verifiable data (Harvey 1991); and (b) deficiencies in content coverage, especially for managerial jobs. The outcomes of such job analysis depend heavily on the DACUM panel. Some other committee with a different set of membership could come up with a different curriculum prescription for ISM. The DACUM process relies on two critical factors for its success. 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 of the DACUM. Also, some instructors in the panel may tend to push the panel toward their own training programs. The second criterion is having a skilled DACUM 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 DACUM chart.

This 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 DACUM and interviews, including the final validation step in which the committee reviewed the feedback from industry and academia. Since DACUM is a cost-effective approach, this technique can be applied even 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 ISM 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.

6. 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) and the reviewers for their comments and suggestions in improving the quality of this publication.

7. 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 199-1, US Department of Justice National Institute of Corrections, NIC Academy, September, 1-3.
- Harvey, Robert J., 1991, Job Analysis. In M. D. Dunnette and L. M. Hough (Eds.), *Handbook of Industrial and Organizational Psychology* (2nd ed., pp. 71-163). 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 - 1 to 5.
- Kim, Ki-Yoon, Na, Hyun-Mi, Kang, Zon-Sik, Kim, Jung-Duck, Sin, Young-Su, Sim, Jong-Cheul, Lee, Sung-Keun, Youn, Ki-Ju, Choi, Jong-Lack, Choi, Jong-Uk, and Hwang, Heu-Sun, 1999, *Job Analysis for Information Security Manager*, Report 99-9-8, Korea Research Institute of Vocational Education and Training.
- Laswell, Barbara S., Simmel, Derek., & Behrens, Sandra G., 1999, *Information Assurance Curriculum and Certification: State of Practice*, Technical Report, Software Engineering Institute, Carnegie Mellon University, 1.
- NIST, 1990, *Simplified Risk Analysis Guidelines*, NISTIR 4387, U.S. Department of Justice.
- Wilson, Mark., de Zafra, Dorothea E., Pitcher, Sadie I., Tressler, John D., and Ippolito, John B., 1998, *Information Technology Security Training Requirements: A Role- and Performance- Based Model*, National Institute of Standards and Technology, U.S. Department of Commerce, 16.