Defining Information Security Management Position Requirements

■ Guidance for Executives and Managers

ISACA®
Serving IT Governance Professionals

ISACA®

With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal®*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 9,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

Disclaimer

ISACA has designed and created *Defining Information Security Management Position Requirements: Guidance for Executives and Managers* (the "Work") primarily as an educational resource for information security managers. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, control professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

Defining Information Security Management Position Requirements: Guidance for Executives and Managers
Printed in the United States of America

Acknowledgments

ISACA wishes to recognize:

Leadership Focus Group
Ken Baylor, Ph.D., CISM, CISSP, Nuance, USA
Robert Coles, CISA, CISM, Merrill Lynch, UK
Sonia DaSilva, CISA, CISM, CGEIT, Memorial Sloan-Kettering Cancer Center, USA
Lee Kushner, LJ Kushner, USA
Hans Joern Lund-Andersen, CISA, CISM, Dong Energy, Denmark
Marc Noble, CISM, CISSP, ISSAP, Federal Communications Commission, USA
John Nugent, Ph.D., CISM, CFE, CPA, DBA, University of Dallas, USA
Michael Raisinghani, Ph.D., CISM, CECC, PMP, Texas Women's University, USA
Marc A. L. J. Vael, Ph.D., CISA, CISM, KPMG, Belgium
Vishnal Vilas Salvi, CISM, HDFC Bank Limited, India

Board of Directors
Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info. SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CFE, CCP, CFSA, FFA, Focus Strategic Group Inc., Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director
Tony Hayes, CPA, Queensland Government, Australia, Director
Jo Stewart-Rattray, CISA, CISM, CSEPS, RSM Bird Cameron, Australia, Director

Security Management Committee
Jo Stewart-Rattray, CISA, CISM, CSEPS, RSM Bird Cameron, Australia, Chair
Manuel Aceves, CISA, CISM, CISSP, Cerberian Consulting, Mexico
Kent Anderson, CISM, Encurve LLC, USA
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd, USA
Yves Le Roux, CISM, CA Inc., France
Mark Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers, USA
Kyeong-Hee Oh, CISA, CISM, Fullbitsoft, Korea
Vernon Poole, CISM, CGEIT, Sapphire Technologies Ltd., UK
Rolf von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany

CISM Certification Board
Evelyn Susana Anton, CISA, CISM, UTE, Venezuela, Chair
Garry James Barnes, CISA, CISM, CISA, Commonwealth Bank of Australia, Australia
Allan Neville Boardman, CISA, CISM, CA, CISSP, JP Morgan Chase, UK
John Randolph Caraway, CISM, CISSP, JP Morgan Chase, USA
James A. Crawford Jr., CISM, CISSP, MSIA, Marine Forces Reserve, USA
Ramses Gallego, CISM, CISSP, SCPM, Entel IT Consulting, Spain
Hitoshi Ota, CISA, CISM, CIA, Mizuho Corporate Bank Ltd., Japan
Smita Dilip Totade, Ph.D., CISA, CISM, FEI, National Insurance Academy, India
Michael Wai-Kee Yung, CISA, CISM, ESD Services Ltd., Hong Kong

Table of Contents

Introduction

As information security has matured into its own discipline, there have been many new career opportunities that have surfaced. Since it has been increasingly difficult to define these job positions and required skills, ISACA and the IT Governance Institute® (ITGI™) have engaged in research to provide members with information that can help them define security position requirements.

As the information security profession has matured, it has been met with increasing business and technical requirements. Enterprises now face myriad regulatory requirements as well as an always present, ever-changing threat profile and the need to manage risk. It is imperative that enterprises recruit professionals with the appropriate skills to ensure that information assets are protected from unauthorized use, systems are available, and the continued integrity of information and processes is assured. It is also imperative that security professionals in leadership positions have the practical security and business experience to be able to address the changing protection needs of the enterprise.

As it currently stands, there is no *de facto* specification defining information security management responsibilities, knowledge or optimal reporting relationships. Many information security positions report to the chief information officer (CIO), others to a chief information security officer (CISO), chief risk officer (CRO) or chief compliance officer (CCO). Job responsibilities differ among enterprises as well. Some enterprises have moved toward a converged security model in which a CSO is responsible for both information and physical security. Others view information security solely as a technology issue. Many enterprises are coming to the conclusion that information security is a business issue that affects an enterprise's overall financial status.

Audience

This report has been prepared to provide a position description and contemporary career path for information security professionals. It is intended to serve as a guide for those involved with information security, including human resource professionals, information security professionals, executives, governing bodies, and boards of directors or trustees.

Because the field of information security is relatively new, originating in the 1970s, many professionals have entered the information security discipline from diverse career paths, including IT, accounting, auditing, law, business operations, engineering, project management and physical security. Due to the various backgrounds that information security professionals bring to their positions, an essential element of this report is a diagram of the various pathways by which these professionals have entered and progressed in information security positions. This diagram (**figure 2**) is provided to summarize and present, in a logical, easy-to-view form, the pathways, levels, roles and functions that accrue to information security professionals and managers in an enterprise.

This report is intended to serve as a practical guide to defining career paths and essential attributes of the information security manager position.

It can be tailored to the specific requirements of an enterprise based on its size, scale, nature, resources, position level and complexity.

Goals and Objectives

This report provides a framework for understanding the many changing and interrelated requirements of the information security manager position and the responsibilities assigned to professionals at various levels in an enterprise. It also identifies the pathways that professionals often take during their careers to reach these positions. The report is intended to help those who are entering the profession from a university program, planning their career or advancing within the profession. It also serves as a guide for those with responsibility for hiring information security practitioners or those who manage, lead or have oversight responsibilities for an information security function.

ISACA Data

The extensive research used in preparing this report includes data collected under the direction of ISACA as part of a comprehensive 2006 global survey of approximately 600 information security professionals holding the Certified Information Security Manager® (CISM®) designation, as well as a working group of information security executives, including more than 100 CISMs. Appendix A lists additional demographic data gathered in the 2006 survey. Additionally, in 2007, ISACA launched its Information Security Career Progression Survey,[1] which generated responses from more than 1,400 CISMs worldwide; those results are reflected in this publication.

The CISM designation is issued by ISACA and is acknowledged by the International Organization for Standardization (ISO) as one of a select group of information security professional certifications receiving worldwide recognition.

Benefits of This Effort

By using this report, the reader will gain a clear understanding of the dynamics and requirements for the information security management position in relation to changing employment needs, the rate and degree of technology change taking place, and how these conditions will impact the role of the information security manager. It will help in defining, refining and updating the requirements for information security management positions, keeping in mind that management skills and abilities may be more critical than technical competencies, particularly in progressing upward within an enterprise.

[1] ISACA, *Information Security Career Progression Survey Results*, USA, 2008

1. Security Within Context

Information security is a business function. As such, it is crucial that information security professionals looking to advance within an enterprise develop sound business skills in addition to functional skills, knowledge and abilities.

In a recent *Computerworld* article, titled "How IT Is Revitalizing Staff Skills,"[2] interviewees pointed out the overwhelming need for cross-functional knowledge and expertise, as well as general business and management abilities, to progress within an enterprise. These interviewees also identified the need for technical professionals to master business skills, knowledge and abilities.

Today it is essential for information security professionals not only to understand the technical issues that are an essential part of their functional role, but also to be able to communicate, interface with and manage others based on sound business management principles and practices.

ISACA's research report titled *Critical Elements of Information Security Program Success*[3] clearly identifies the need for executive and senior management and the information security manager to forge a relationship that will relay a consistent message with regard to the priority the enterprise places on protecting valuable information and assets.

To properly align business risks and information security solutions, a cooperative dialog between business areas and information security experts is necessary. However, to be successful, the dialog must be supported by visible and consistent action. That action is best represented by the establishment and consistent implementation of company policies and standards. The ISACA report indicates that, without the active participation of executive management in the implementation and management of an information security strategy, progress will be eroded by inconsistent compliance with policies, resulting in a false sense of comfort regarding asset protection.

Conflicts among day-to-day priorities affect the quality and consistency of information asset protection. These conflicts must be dealt with in a coordinated manner. To ensure that associated risks are taken seriously by every employee and agent of the enterprise, executive and senior management must become visibly interested in ensuring the information security program's success within their enterprises.

Another key finding of the report is that information security professionals are beginning to recognize that they need to develop a solid understanding of the business as their role becomes more visible in the enterprise. Their decisions demand business risk justification, and the enterprise's dependence on technology drives increased interaction with their legal and compliance counterparts in the enterprise.

[2] Robb, D; "How IT Is Revitalizing Staff Skills," *Computerworld*, USA, February 2007
[3] ISACA, *Critical Elements of Information Security Program Success*, USA, 2005

Role of Information Security Managers

It seems the information security manager role is constantly evolving—not only are the paths to get to an information security management position different, but the roles and responsibilities among information security professionals differ as well.

In *Information Security Career Progression Survey Results*, CISMs reported that their job activities changed significantly from their previous to their present job. CISMs are seeing a decrease in technical responsibilities and a significant increase in areas such as security program management, risk management and compliance. Appendix B demonstrates the amount of time CISMs report spending in the certification's five job practice areas. **Figure 1** presents the percentage of CISMs who perform certain activities. The figure shows that a much higher percentage of CISMs are responsible for business functions (shown in **bold**) in their current role than they were in their previous role. Mapping information security to the business has become a top priority.

Figure 1—Percentage of CISMs Responsible for Security Activities

Rank	Current Position	Percent	Prior Position	Percent
1	**Risk management**	76.6	Data security	56.6
2	**Security program management**	74.0	**Risk management**	54.8
3	Data security	70.7	Network security	53.5
4	**Policy creation and maintenance**	65.3	**Security program management**	49.0
5	**Regulatory compliance**	63.4	**Policy creation and maintenance**	48.8
6	**Security project management**	59.6	**Business continuity/disaster recovery**	45.8
7	Incident management	58.5	System and application security	45.2
8	Network security	57.3	Security architecture	45.1
9	**Business continuity/disaster recovery**	56.1	Incident management	44.8
10	Security architecture	55.9	**Security project management**	44.8

Source: ISACA, *Information Security Career Progression Survey Results*, USA, 2008

Some current common job requirements for information security managers include:

- Overseeing the establishment, implementation and adherence to policies and standards that guide and support the terms of the information security strategy
- Communicating with executive management to ensure support for the information security program
- Overseeing and conducting risk management activities (risk assessment, gap analysis, business impact analysis, etc.) to help the enterprise reach an acceptable level of risk
- Advising and making recommendations regarding appropriate personnel, physical and technical security controls
- Managing the information security incident management program to ensure the prevention, detection, containment and correction of security breaches
- Reporting appropriate metrics to executive management
- Participating in resolving problems with security violations

- Creating an enterprisewide information security education and awareness campaign
- Coordinating the communication of the information security awareness campaign to all members of the enterprise
- Coordinating with vendors, auditors, executive management and user departments to enhance information security

To stay current with ever-changing roles and responsibilities, continuous education, certification and professional development are musts. Information security has matured beyond a technical response role, and executives and senior management are beginning to recognize this change.

To continue to move the profession forward, information security managers must be able to demonstrate the value of information security to the enterprise. Effective communication of the value of the security program requires the information security manager not only to understand technology and solutions, but also, and more important, to be competent in areas traditionally thought of as business skills. Communication (written and verbal), organizational, and financial and management skills are all highly important when communicating with enterprise leaders.

2. Position Description

According to the *Certified Information Security Manager Job Practice Analysis Study*,[4] responding CISMs expect that the information security manager will have a more central role in business within the next three years. Additionally, respondents expect to see an increased emphasis on governance, as well as a heightened focus on risk management and incident management.

Respondents to the practice analysis survey also indicated that there were many knowledge areas and skills that they needed to acquire within the last year. These skills and knowledge areas include:

- Business skills
- Management skills
- Deeper knowledge of regulatory/compliance requirements
- Sarbanes-Oxley knowledge
- Risk assessment/risk management skills
- Forensics
- Security, including information security management, physical security and network security

To assist enterprises in choosing highly skilled professionals for information security management positions, a number of professional certifications have been created. ISACA launched its CISM certification in 2002. The certification is designed for information security managers possessing at least five years of experience and both security and business skills.

The CISM exam covers five job practice areas that focus on different information security task and knowledge statements. The task statements represent what an information security professional should be able to do, and the knowledge statements (see appendix C) represent what the information security manager should know to perform the tasks.

Information Security Governance

The first job practice area identified by information security managers as essential to their role is information security governance. As governance is clearly a business issue, it is in this category that the information security manager is expected to have effective skills in working with executives and realizing how to demonstrate the value of information security to the enterprise. The following are eight key task statements in the information security governance area:[5]

- Develop an information security strategy aligned with business goals and objectives.
- Align information security strategy with corporate governance.
- Develop a business case justifying investment in information security.
- Identify current and potential legal and regulatory requirements affecting information security.
- Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.

[4] ISACA, *Certified Information Security Manager Job Practice Analysis Study*, USA, 2006
[5] ISACA, *CISM Review Manual 2008*, USA, 2008

- Obtain senior management commitment to information security.
- Define roles and responsibilities for information security throughout the organization.
- Establish internal and external reporting and communication channels that support information security.

The task statements demonstrate an alignment between the information security program and the needs of the business. To effectively manage the information security program, the manager needs to have the business knowledge to perform the previously mentioned tasks. The manager must possess communication skills to gain support from executives and must be able to understand financial reports to clearly see the business drivers. The manager also needs to be able to work effectively with other areas, including legal and audit to identify potential regulatory concerns, human resources and heads of functional business units to define responsibilities as they pertain to information security.

Risk Management

Information security risk management is the second area of critical information security management responsibility contained within the CISM job practice areas. This area represents the entire cycle of managing risk in an enterprise, from assessment through mitigation. Here, information security managers need to conduct risk assessments, understand and clearly communicate the possible impact to the business, and recommend controls for mitigation.

Tasks critical to handling risk management effectively include the following:

- Establish a process for information asset classification and ownership.
- Implement a systemic and structured information risk assessment process.
- Ensure that business impact assessments are conducted periodically.
- Ensure that threat and vulnerability evaluations are performed on an ongoing basis.
- Identify and periodically evaluate information security controls and countermeasures to mitigate risk to acceptable levels.
- Integrate risk, threat and vulnerability identification and management into life cycle processes (e.g., development and procurement).
- Report significant changes in information risk to appropriate levels of management for acceptance on both a periodic and an event-driven basis.

The seven task statements listed represent a wide range of knowledge. Information security managers not only must have a thorough knowledge of threats, vulnerabilities and possible exposures, but also must understand methods to assess risk, possible mitigation strategies, methods of conducting a gap analysis and business impact analysis, and have solid knowledge of security controls and countermeasures. Most important, to make any decisions regarding treatment of risk, the information security manager must know how to communicate with executive management regarding the risk tolerance of the enterprise and must be able to contribute to the identification and management of risk at an enterprise level.

Information Security Program Development

Information security program development is the third essential capability critical to the information security manager role. When creating an information security program, it is critical for information security managers to align the program with enterprise goals and demonstrate value. Information security managers need to have a strong understanding of people, process and technology to effectively achieve business objectives.

Information security managers should be able to complete the following 11 tasks in information security program development:

- Develop and maintain plans to implement the information security strategy.
- Specify the activities to be performed within the information security program.
- Ensure alignment between the information security program and other assurance functions (e.g., physical, human resources, quality, IT).
- Identify internal and external resources (e.g., finances, people, equipment, systems) required to execute the security program.
- Ensure the development of information security architectures (e.g., people, processes, technology).
- Establish, communicate and maintain information security policies that support the security strategy.
- Design and develop a program for information security awareness, training and education.
- Ensure the development, communication and maintenance of standards, procedures and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
- Integrate information security requirements into the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities (e.g., development, employment, procurement).
- Develop a process to integrate information security controls into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties).
- Establish metrics to evaluate the effectiveness of the information security program.

The information security program development tasks required of the information security manager clearly highlight the need for individuals who are able to understand business objectives and who have strong communication skills. Developing an effective security program depends on the manager's abilities to understand the strategy and goals of the enterprise and to work with executives and functional business unit leaders to integrate security into enterprise culture.

Information Security Program Management

Information security program management is the fourth CISM job practice area. Its focus is to effectively manage the information security program by bringing together human, physical and financial resources to help achieve business objectives.

There are nine tasks within this job practice area that the information security manager should be able to complete effectively:

- Manage internal and external resources (e.g., finances, people, equipment, systems) required to execute the information security program.
- Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
- Ensure the performance of contractually agreed (e.g., with joint ventures, outsourced providers, business partners, customers, third parties) information security controls.

- Ensure that information security is an integral part of the systems development processes and acquisition processes.
- Ensure that information security is maintained throughout the organization's processes (e.g., change control, mergers and acquisitions) and life cycle activities.
- Provide information security advice and guidance (e.g., risk analysis, control selection) in the organization.
- Provide information security awareness, training and education (e.g., business process owners, users, information technology) to stakeholders.
- Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
- Ensure that noncompliance issues and other variances are resolved in a timely manner.

As can be seen by the tasks listed, communication skills are critical to program management. Information security managers need to develop and report appropriate metrics to demonstrate value to senior management. Information security managers also must be able to communicate on a technical level with IT specialists, business unit leaders and employees, all of whom share responsibilities for the protection of valuable information assets.

Incident Management and Response

The final job practice area covered is incident management and response. Incident management is defined as the process of developing and maintaining the capability to manage incidents within an enterprise so that exposure can be contained and recovery achieved within a specified time objective. Incidents can include the misuse of computing assets, information disclosure or events that threaten the continuance of business processes. There are 10 critical tasks at which information security managers should be proficient in this practice area:

- Develop and implement processes for preventing, detecting, identifying, analyzing and responding to information security incidents.
- Establish escalation and communication processes and lines of authority.
- Develop plans to respond to and document information security incidents.
- Establish the capability to investigate information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
- Develop a process to communicate with internal parties and external organizations (e.g., media, law enforcement, customers).
- Integrate information security incident response plans with the organization's disaster recovery and business continuity plan.
- Organize, train and equip teams to respond to information security incidents.
- Periodically test and refine information security incident response plans.
- Manage the response to information security incidents.
- Conduct reviews to identify causes of information security incidents, develop corrective actions and reassess risk.

The incident management and response job practice area requires information security managers to identify, analyze, manage and respond to a disruption to, or failure in, information processing functions.

3. Career Progression

Information security managers need a wide range of skills to be successful in their roles. Some of these skills pertain to management, risk management, technology, communication, project management, organization and leadership. With an increased focus on business skills and soft skills that may be hard to measure, it is recommended that any enterprise hiring an information security manager look for an individual who has experience in the five CISM job content areas.

It is important to note that hiring outsiders is not always the only option. Enterprises often have existing employees with critical skills. Information security professionals may enter an enterprise in one area and acquire additional skills that allow them to progress to another.

Figure 2 illustrates the numerous career pathways by which an information security manager may progress in an enterprise. It demonstrates the typical information security progression and shows how professionals may move horizontally, diagonally and vertically as they progress in their careers. This figure also highlights the fact that there are many backgrounds and means through which managers of information security gain knowledge, certification, training and experience.

The rise from an entry-level position to a C-level position may take many paths; in fact, this is precisely the pattern seen today when surveying CISM certification holders across the globe. These professionals entered from numerous functional areas and progressed up the corporate ladder in both vertical and horizontal patterns, often moving diagonally as well. Since blended technical and managerial skills are needed as one moves higher in an enterprise, it is believed this pattern will remain relevant in the future.

The skill sets required by today's information security managers are not always easy to measure. Employers need a basis on which to evaluate employees for progression and outside candidates for positions. Bloom's taxonomy[6] offers enterprises a scale with which to identify whether potential job holders have the necessary skill sets to perform the role of information security manager.

Bloom identified six levels within the cognitive domain, from the lowest level—simple recall or recognition of facts—through increasingly more complex and abstract mental levels, to the highest order, which is classified as evaluation.Verb examples that represent intellectual activity on each level are listed in **figure 3**.

Figure 4 takes a closer look at the competencies for the information security manager position, adapted from Bloom's six levels of learning. The level of competence for different corporate levels is suggested for each of Bloom's competencies: knowledge, comprehension, application, analysis, synthesis and evaluation. Competency requirements in the various areas may be met by having professionals with different strengths on the team.

[6] Bloom, B; *Taxonomy of Educational Objectives*, Allyn and Bacon, USA, 1984

Figure 2—Typical Information Security Progression and Management Model

Board of Directors Information Security/Assurance Committee

C-level Cross-functional Team

Career Levels

Level	Management		Technology	Architecture	Assurance	Legal/Risk Management/ Privacy
Senior executive (C-level)	**CIO**	**COO**	**CTO CISO CArO**		**CAO**	**GC CRO CPO**
Manager/ director	Operations consulting	Development/systems and infrastructure information security			Internal audit	Information risk/privacy consulting
Expert	Principal IT consultant	Senior IT systems professional	Senior IT development engineer	Senior IT architect	Senior information security auditor	Principal IT consultant
Specialist, manager	Product/program/project manager, team leader, account sales manager					
Specialist, technical	Security consultant, business analyst	Security product manager	Security designer	Security systems professional	Security auditor	Information risk consultant
Entrant	Analyst		Developer	Security designer trainee	Security systems trainee	Security auditor trainee

Career movement through the C-level may be vertical, horizontal and/or diagonal.

Source: Adapted from Lynas, David; John Sherwood; "Professionalism in Information Security: A Framework for Competency Development," 12th Annual COSAC Conference, UK, 2005

C-level Key:

CIO = Chief information officer	CAO = Chief assurance officer
COO = Chief operating officer	GC = General counsel
CTO = Chief technology officer	CRO = Chief risk officer
CISO = Chief information security officer	CPO = Chief privacy officer
CArO = Chief architecture officer	

Enterprises looking to promote or hire an information security manager may find the competencies helpful in determining qualifications and position requirements.

A manager of information security needs extensive, in-depth knowledge of a variety of areas. In many cases, this level of knowledge will not be found in a single person, especially early in a career. Therefore, it is likely that a balancing of skills across several professionals will be required in larger enterprises, with those who have a broader and deeper grasp of the required knowledge rising to the more senior positions. Because technology is changing so rapidly, continuous training and education are required.

Figure 3—Technical Competencies Based on Bloom's Taxonomy

	Competency Level	Skill Demonstrated	Behavioral Verb Examples
1	Knowledge	• Observe and recall information. • Show knowledge of facts. • Show knowledge of major ideas. • Demonstrate mastery of subject matter. • Conduct research to find information.	List, define, tell, describe, identify, show, label, collect, examine, tabulate, quote, name, find, identify
2	Comprehension	• Understand information. • Grasp meaning. • Translate knowledge into new context. • Interpret facts. • Compare and contrast. • Infer causes. • Predict consequences.	Summarize, explain, interpret, contrast, predict, associate, distinguish, estimate, differentiate, discuss, extend, order, group
3	Application	• Use information wisely. • Use methods, concepts and theories in new situations. • Solve problems using the required skills or knowledge.	Apply, demonstrate, calculate, complete, illustrate, show, solve, examine, modify, relate, change, classify, experiment, discover
4	Analysis	• Identify patterns. • Organize parts. • Recognize hidden meanings. • Identify components.	Analyze, separate, order, connect, classify, arrange, divide, compare, select, infer
5	Synthesis	• Use old ideas to create new ones. • Generalize from given facts. • Relate knowledge from several areas. • Make predictions and draw conclusions.	Combine, integrate, modify, rearrange, substitute, plan, create, build, design, invent, compose, formulate, prepare, generalize, rewrite
6	Evaluation	• Compare and discriminate between ideas. • Assess value of theories and presentations. • Make choices based on reasoned argument. • Verify value of evidence. • Recognize subjectivity.	Assess, evaluate, decide, rank, grade, test, measure, recommend, convince, select, judge, discriminate, support, conclude

Source: Bloom, Benjamin; *Taxonomy of Educational Objectives*, Allyn and Bacon, USA, 1984

Figure 4—Competencies for a Manager of Information Security

Domain	Knowledge		Comprehension		Application		Analysis		Synthesis		Evaluation	
Level/ category	Bus.	Sec.	Bus.	Sec.	Bus.	Sec.	Bus.	Sec.	Bus.	Sec.	Bus.	Sec.
C-level executive	M	M	M	M	M	M	M	M	M	M	M	M
Director	M	M	M	M	M	M	M	M	M	M	M	M
Manager	C	M	M	M	M	M	M	M	C	C	C	C
Technical expert	C	M	C	M	C	M	C	M	U	M	U	M
Technical specialist	U	M	U	M	U	M	U	M	U	C	U	C
Technical analyst	U	C	U	C	U	C	U	C	U	C	U	C

Source: University of Dallas Center for Information Assurance, 2007

Table Key
Bus. = Business knowledge
Sec. = Information security knowledge
M = Complete mastery
C = Some competency
U = Basic understanding

Basis for Skills

Professional certifications and education play an important role in developing skills and demonstrating one’s professionalism and commitment to maintain a professional standing.

Education can be provided in a formal education setting such as a college or university where undergraduate, graduate and doctoral programs now exist for information security managers, or it may come in the form of professional education at conferences, seminars and workshops.

Professional certification can be very valuable in demonstrating information security management knowledge and experience because it requires candidates to pass an exam that draws on their competencies in information security. CISM is a highly respected information security management certification that requires candidates to pass a rigorous exam and possess five years of information security management experience, and then earn continued professional education (CPE) hours to maintain the certification.

Conclusion

The roles, responsibilities and relationships that information security managers must fulfill are large, growing, complex and sometimes conflicted, but they are uniform across the globe. Their challenge, according to the CISM job practice analysis survey,[7] is that they must become adept at understanding business issues and fundamentals as well as managing and working with other technical professionals if they wish to progress in their career. There is so much to know and keep up with in relation to changing technology; thus, training, certification and continuing education are imperative.

It was also determined from the CISM job practice analysis survey that many managers of information security moved into their position via different career paths and educational backgrounds. This has worked well as it builds a lattice of skills, experience, education, training and certification enhancing the overall security profile of an enterprise. For this reason, it is believed that upward movement in the information security manager's career chain will take different paths, with some professionals progressing in a vertical channel and others from a horizontal position, and some transferring from a purely technical position to a more managerial role and *vice versa*.

Finally, for true enterprise security to be effective, there must be buy-in at the top. This means that information security must be enmeshed in corporate governance and must have the participation and support of the board and senior executives.

Creating a culture supportive of information security is just one of many challenges that information security managers face today, but the appropriate combination of education and experience will help equip them to meet those challenges.

[7] ISACA, *Certified Information Security Manager Job Practice Analysis Study*, USA, 2006

Appendix A—Professional Profile of CISM Job Practice Analysis Survey Participants

The following statistics represent demographic data derived from ISACA's 2006 *Certified Information Security Manager Job Practice Analysis Study*:

- 70 percent of respondents had six to 15 years of experience as an information security manager.
- 59 percent came from four sectors: banking (16 percent), consulting (23 percent), finance (7 percent) and government/national (13 percent).
- 83 percent were male.
- 77 percent held a bachelor's degree or higher (38 percent had a bachelor's degree and 39 percent also held a master's degree).
- While all respondents held the CISM credential, more than 73 percent had an additional certification (40 percent had CISSP, 33 percent had CISA, 33 percent had others).
- 65 percent held one of the following three titles: CISO (13 percent), director of information security (13 percent) or manager of information security (39 percent).
- 94 percent had been certified since 2003.
- 33 percent were employed in firms with 1,500 to 9,999 employees (other responses were spread evenly in a bell curve).
- 62 percent had full-time security staffs of fewer than 25 people (39 percent had a staff of zero to five, 17 percent had a staff of six to 10, and 16 percent had a staff of 11 to 25).

Note: Percentages have been rounded to whole numbers.

Source: ISACA, *Certified Information Security Manager Job Practice Analysis Study*, USA, 2006, p. 19-27

Appendix B—Tasks and Knowledge Scores

Figure 5 represents the responses of CISMs polled in the 2006 job practice analysis study. CISMs responded with the percentage of time they spent managing activities in each of the CISM job content areas and also the criticality of the job content areas in their job. The criticality mean is an average of all scores, based on a linear scale from 1 to 5; 1 indicates the least critical and 5 indicates the most critical.

Figure 5—Descriptive Statistics for Content Area on the CISM Exam

Content Areas on CISM Exam	Percent of Time	Criticality Mean
Information security governance	22.0	3.5
Information security risk management	21.5	3.6
Information security program development	17.6	3.4
Information security program management	24.0	3.5
Incident management and response	13.6	3.4
Other	1.2	–

Source: ISACA, *Certified Information Security Manager Job Practice Analysis Study*, USA, 2006, p. 29

Appendix C—Knowledge Statements for Each CISM Job Content Area

(Source: ISACA, *CISM Review Manual 2008*, USA, 2008)

Area 1: Information Security Governance

KS1.1 Knowledge of the business goals and objectives

KS1.2 Knowledge of information security concepts

KS1.3 Knowledge of the components that comprise an information security strategy (e.g., people, processes, technologies, architecture)

KS1.4 Knowledge of the relationship between information security and business functions

KS1.5 Knowledge of the scope and charter of information security governance

KS1.6 Knowledge of concepts of corporate and information security governance

KS1.7 Knowledge of methods of integrating information security governance into the overall enterprise governance framework

KS1.8 Knowledge of budgetary planning strategies and reporting methods

KS1.9 Knowledge of methodologies for business case development

KS1.10 Knowledge of the types and impact of internal and external drivers (e.g., technology, business environment, risk tolerance) that may affect organizations and information security

KS1.11 Knowledge of regulatory requirements and their potential business impact from an information security standpoint

KS1.12 Knowledge of common liability management strategies and insurance options (e.g., crime or fidelity insurance, business interruptions)

KS1.13 Knowledge of third-party relationships and their impact on information security (e.g., mergers and acquisitions, partnerships, outsourcing)

KS1.14 Knowledge of methods used to obtain senior management commitment to information security

KS1.15 Knowledge of the establishment and operation of an information security steering group

KS1.16 Knowledge of information security management roles, responsibilities and general organizational structures

KS1.17 Knowledge of approaches of linking policies to enterprise business objectives

KS1.18 Knowledge of generally accepted international standards for information security management

KS1.19 Knowledge of centralized and distributed methods of coordinating information security activities

KS1.20 Knowledge of methods for establishing reporting and communication channels throughout an organization

Area 2: Information Security Risk Management

KS2.1 Knowledge of required components for establishing an information security classification schema consistent with business objectives (including the identification of assets)

KS2.2 Knowledge of the components of information ownership schema (including drivers of the schema, such as roles and responsibilities)

KS2.3 Knowledge of information threats, vulnerabilities and exposures

KS2.4 Knowledge of information resource valuation methodologies

KS2.5 Knowledge of risk assessment and analysis methodologies (including measurability, repeatability and documentation)

KS2.6 Knowledge of the factors used to determine risk reporting frequency and requirements

KS2.7 Knowledge of quantitative and qualitative methods used to determine sensitivity and criticality of information resources and the impact of adverse events on the business

KS2.8 Knowledge of baseline modeling and its relationship to risk-based assessments of control requirements

KS2.9 Knowledge of security controls and countermeasures

KS2.10 Knowledge of methods of analyzing the effectiveness of information security controls and countermeasures

KS2.11 Knowledge of risk mitigation strategies used in defining security requirements for information resources

KS2.12 Knowledge of gap analysis to assess the current state against generally accepted standards of good practice for information security management

KS2.13 Knowledge of cost-benefit analysis techniques for mitigating risks to acceptable levels

KS2.14 Knowledge of life-cycle-based risk management principles and practices

Area 3: Information Security Program Development

KS3.1 Knowledge of methods to interpret strategies into manageable and maintainable plans for implementing information security

KS3.2 Knowledge of the activities required within an information security program

KS3.3 Knowledge of methods for managing the implementation of the information security program

KS3.4 Knowledge of planning, designing, developing, testing and implementing information security controls

KS3.5 Knowledge of methods to align information security program requirements with those of other assurance functions (e.g., physical, human resources, quality, IT)

KS3.6 Knowledge of how to identify internal and external resources and skills requirements (e.g., finances, people, equipment, systems)

KS3.7 Knowledge of resource and skills acquisition (e.g., project budgeting, employment of contract staff, equipment purchase)

KS3.8 Knowledge of information security architectures (e.g., logical architecture and physical architectures) and their deployment

KS3.9 Knowledge of security technologies and controls (e.g., cryptographic techniques, access controls, monitoring tools)

KS3.10 Knowledge of the process for developing information security policies that meet and support enterprise business objectives

KS3.11 Knowledge of content for information security awareness, training and education across the enterprise (e.g., general security awareness, writing secure code, operating system controls)

KS3.12 Knowledge of methods to identify activities to close the gap between proficiency levels and skill requirements

KS3.13 Knowledge of activities to foster a positive security culture and behavior

KS3.14 Knowledge of the uses of and differences among policies, standards, procedures, guidelines and other documentation

KS3.15 Knowledge of the process for linking policies to enterprise business objectives

KS3.16 Knowledge of methods to develop, implement, communicate and maintain information security policies, standards, procedures, guidelines and other documentation

KS3.17 Knowledge of integrating information security requirements into organizational processes (e.g., change control, mergers and acquisition)

KS3.18 Knowledge of life cycle methodologies and activities (e.g., development, employment, procurement)

KS3.19 Knowledge of processes for incorporating security requirements into contracts (e.g., with joint ventures, outsourced providers, business partners, customers, third parties)

KS3.20 Knowledge of methods and techniques to manage third-party risks (e.g., service level agreements, contracts, due diligence, suppliers, subcontractors)

KS3.21 Knowledge of the design, development and implementation of information security metrics

KS3.22 Knowledge of certifying and accrediting the compliance of business applications and infrastructure to business needs

KS3.23 Methods for ongoing evaluation of the effectiveness and applicability of information security controls (e.g., vulnerability testing, assessment tools)

KS3.24 Knowledge of methods of tracking and measuring the effectiveness and currency of information security awareness, training and education

KS3.25 Knowledge of methods of sustaining the information security program (e.g., succession planning, allocation of jobs, documentation of the program)

Area 4: Information Security Program Management

KS4.1 Knowledge of interpreting and implementing information security policies

KS4.2 Knowledge of information security administrative processes and procedures (e.g., access controls, identity management, remote access)

KS4.3 Knowledge of methods for implementing and managing the enterprise's information security program in agreement with third parties (e.g., trade partners, contractors, joint venture partners, outsourcing providers)

KS4.4 Knowledge of methods for managing the information security program through security service providers

KS4.5 Knowledge of information-security-related contract provisions (e.g., right to audit, confidentiality nondisclosure)

KS4.6 Knowledge of methods to define and monitor security requirements in service level agreements

KS4.7 Knowledge of methods and approaches to providing continuous monitoring of security activities in the enterprise's infrastructure and business applications

KS4.8 Knowledge of management metrics to validate the information security program investment (e.g., data collection, periodic review, key performance indicators)

KS4.9 Knowledge of methods of testing the effectiveness and applicability of information security controls (e.g., penetration testing, password cracking, social engineering, assessment tools)

KS4.10 Knowledge of change and configuration management activities

KS4.11 Knowledge of the advantages/disadvantages of using internal/external assurance providers to perform information security reviews

KS4.12 Knowledge of due diligence activities, reviews and related standards for managing and controlling access to information

KS4.13 Knowledge of external vulnerability reporting sources for information on potential impacts on information security in applications and infrastructure

KS4.14 Knowledge of events affecting security baselines that may require risk reassessments and changes to information security program elements

KS4.15 Knowledge of information security problem management practices

KS4.16 Knowledge of reporting requirements of systems and infrastructure security status

KS4.17 Knowledge of general line management techniques, including budgeting (e.g., estimating, quantifying, trade-offs), staff management (e.g., motivating, appraising, objective setting) and facilities (e.g., obtaining and using equipment)

Area 5: Incident Management and Response

KS5.1 Knowledge of the components of an incident response capability

KS5.2 Knowledge of disaster recovery planning and business continuity planning

KS5.3 Knowledge of information incident management practices

KS5.4 Knowledge of disaster recovery testing for infrastructure and critical business applications

KS5.5 Knowledge of events that trigger incident response

KS5.6 Knowledge of containing damage

KS5.7 Knowledge of notification and escalation processes for effective security management

KS5.8 Knowledge of the role of individuals in identifying and managing security incidents

KS5.9 Knowledge of crisis communication

KS5.10 Knowledge of methods of identifying business resources essential to recovery

KS5.11 Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams

KS5.12 Knowledge of forensic requirements for collecting and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody)

KS5.13 Knowledge used to document incidents and subsequent actions

KS5.14 Knowledge of internal and external reporting requirements

KS5.15 Knowledge of postincident review practices and investigative methods to identify causes and determine corrective actions

KS5.16 Knowledge of techniques for quantifying damages, costs and other business impacts arising from security incidents

KS5.17 Knowledge of the recovery time objective (RTO) and its relationship to business continuity and contingency planning objectives and processes

References

Bloom, B.; *Taxonomy of Educational Objectives*, Allyn and Bacon, USA, 1984

Lynas, D.; J. Sherwood; "Professionalism in Information Security: A Framework for Conpetency Development," 12th Annual COSAC Conference, UK, 2005

Robb, D.; "How IT Is Revitalizing Staff Skills," *Computerworld*, USA, February 2007

ISACA, *Certified Information Security Manager Job Practice Analysis Study*, USA, 2006

ISACA, *CISM Review Manual 2008*, USA, 2008

ISACA, *Critical Elements of Information Security Program Success*, USA, 2005

ISACA, *Information Security Career Progression Survey Results*, USA, 2008

Other Publications

Many publications issued by the IT Governance Institute® (ITGI™) and ISACA contain detailed assessment questionnaires and work programs. For further information, please visit *www.isaca.org/bookstore* or e-mail *bookstore@isaca.org*.

Security

- *Cybercrime: Incident Response and Digital Forensics*, 2005
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*, 2006
- *Information Security Governance: Guidance for Information Security Managers*, 2008
- *Information Security Harmonisation—Classification of Global Guidance*, 2005
- *Managing Enterprise Information Integrity: Security, Control and Audit Issues*, 2004
- *Security Awareness: Best Practices to Serve Your Enterprise*, 2005
- *Stepping Through the InfoSec Program*, 2007

Assurance

- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008
- *Stepping Through the IS Audit, 2nd Edition*, 2004

ERP Series:

- *Security, Audit and Control Features Oracle® E-Business Suite: A Technical and Risk Management Reference Guide, 2nd Edition*, 2006
- *Security, Audit and Control Features PeopleSoft®: A Technical and Risk Management Reference Guide, 2nd Edition*, 2006
- *Security, Audit and Control Features SAP®R/3®: A Technical and Risk Management Reference Guide, 2nd Edition*, 2005

Specific Environments:

- *Electronic and Digital Signatures: A Global Status Report*, 2002
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment*, 2004
- *Linux: Security, Audit and Control Features*, 2005
- *Managing Risk in the Wireless LAN Environment: Security, Audit and Control Issues*, 2005
- *Oracle® Database Security, Audit and Control Features*, 2004
- *OS/390—z/OS: Security, Control and Audit Features*, 2003
- *Risks of Customer Relationship Management: A Security, Control and Audit Approach*, 2003
- *Security Provisioning: Managing Access in Extended Enterprises*, 2002
- *Virtual Private Network—New Issues for Network Security*, 2001

IT Governance

- *Board Briefing on IT Governance, 2nd Edition*, 2003
- *Identifying and Aligning Business Goals and IT Goals*, 2008
- *IT Governance Global Status Report—2008*, 2008
- *Understanding How Business Goals Drive IT Goals*, 2008

CobiT and Related Publications

- CobiT® 4.1, 2007
- *CobiT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, 2007
- *CobiT® Quickstart™, 2nd Edition*, 2007
- *CobiT® Security Baseline™, 2nd Edition*, 2007
- *IT Assurance Guide: Using CobiT®*, 2007
- *IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance*, 2007
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, 2006
- *IT Governance Implementation Guide: Using CobiT® and Val IT™, 2nd Edition*, 2007

CobiT Mapping Series:

- *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, 2008
- *CobiT® Mapping: Mapping of CMMI® for Development V1.2 With CobiT® 4.0*, 2007
- *CobiT® Mapping: Mapping of ISO/IEC 17799:2000 With CobiT® 4.0, 2nd Edition*, 2006
- *CobiT® Mapping: Mapping of ISO/IEC 17799:2005 With CobiT® 4.0*, 2006
- *CobiT® Mapping: Mapping of ITIL V3 With CobiT® 4.1*, 2008
- *CobiT® Mapping: Mapping of NIST SP800-53 With CobiT® 4.1*, 2007
- *CobiT® Mapping: Mapping of PMBOK With CobiT® 4.0*, 2006
- *CobiT® Mapping: Mapping of PRINCE2 With CobiT® 4.0*, 2007
- *CobiT® Mapping: Mapping of SEI's CMM for Software With CobiT® 4.0*, 2006
- *CobiT® Mapping: Mapping of TOGAF 8.1 With CobiT® 4.0*, 2007
- *CobiT® Mapping: Overview of International IT Guidance, 2nd Edition*, 2006

IT Governance Domain Practices and Competencies:

- *Governance of Outsourcing*, 2005
- *Information Risks: Whose Business Are They?*, 2005
- *IT Alignment: Who Is in Charge?*, 2005
- *Measuring and Demonstrating the Value of IT*, 2005
- *Optimising Value Creation From IT Investments*, 2005

Val IT:

- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*, 2008
- *Enterprise Value: Governance of IT Investments, The Business Case*, 2006
- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, 2008
- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 Extract*, 2008

ISACA®
Serving IT Governance Professionals

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*