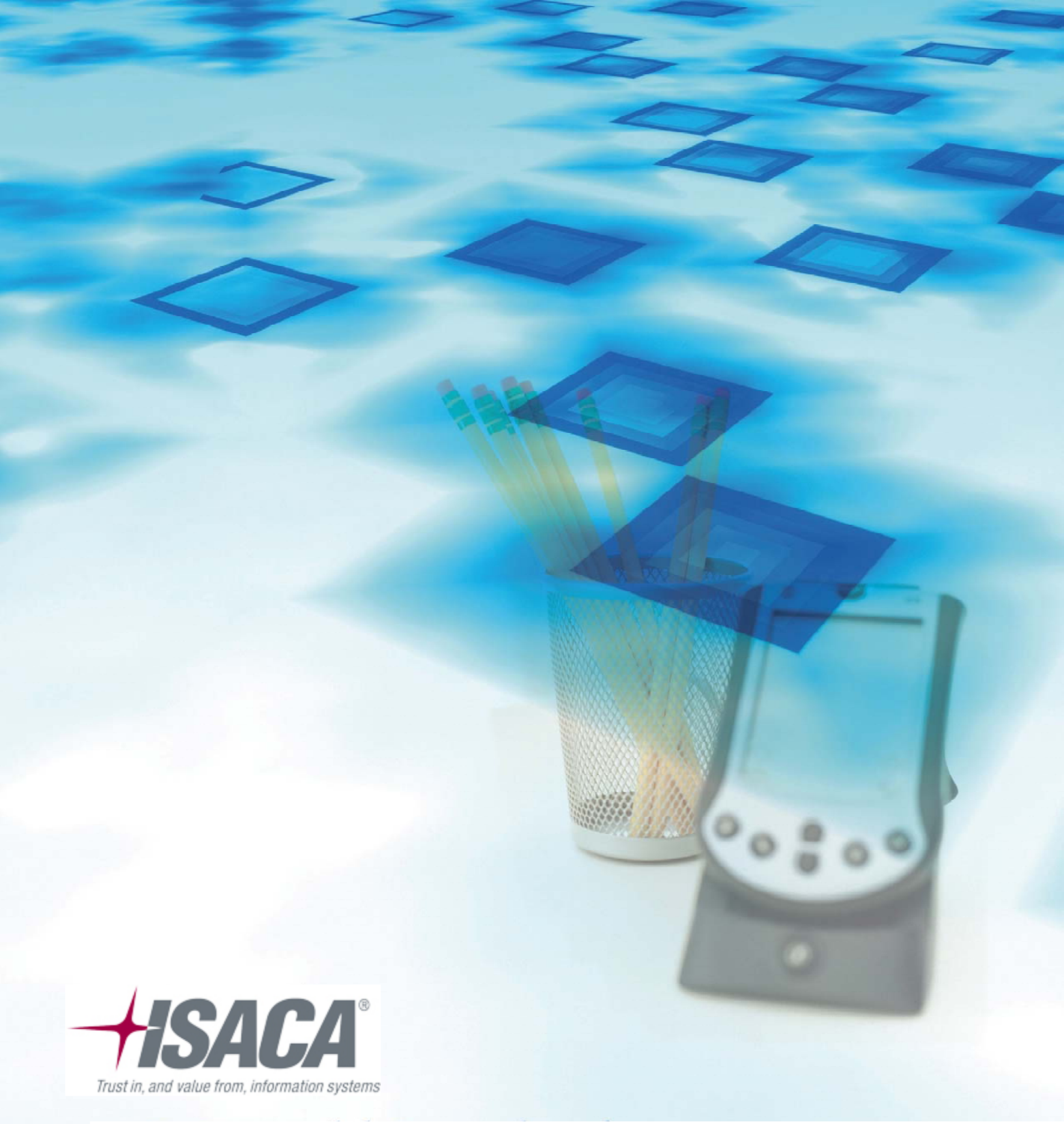

ISACA®
Trust in, and value from, information systems

ISACA® Model Curriculum for Information Security Management, 2nd Edition

ISACA®
With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created *ISACA® Model Curriculum for Information Security Management, 2nd Edition* (the "Work"), primarily as an educational resource for security and governance professionals. 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, security and governance professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

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

ISACA Model Curriculum for Information Security Management, 2nd Edition

Acknowledgments

ISACA wishes to recognize:

ISACA Board of Directors

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

Knowledge Board

Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, USA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

Academic Program Subcommittee

Krishna Seeburn, Ph.D., CFE, CIA, CISSP, PMP, University of Technology, Mauritius, Chairman
Shahriar (Shaun) Aghili, CISA, CFE, CIA, CISSP, CMA, Concordia University College of Alberta, Canada
Sharon Finney, CISM, CISSP, Adventist Health System, USA
Graham Gal, Ph.D., University of Massachusetts, USA
Joshua Onome Imoniana, Ph.D., CGEIT, Universidade Presbiteriana Mackenzie, Brazil
Kameswara Rao Namuduri, Ph.D., CISA, CISM, CISSP, University of North Texas, USA
Vincent Orrico, CISA, CGEIT, CRISC, CBCLA, CBCP, CISSP, PMP, Cushman & Wakefield, USA
Mark D. Phillips, CISA, CIA, Duke University, USA
Kumar Srikanteswaran, CISA, CMA, PMP, Senior Business Consultant, India
Lolita E. Vargas-DeLeon, CISA, CIA, CPA, MIBA, USA

ISACA and IT Governance Institute Affiliates and Sponsors

American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association (ISSA)
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
GRC Solutions Inc.
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

Table of Contents

1. Background

ISACA History

The evolution of information technology (IT) affects the business environment in many significant ways. It has changed business practices, reduced costs and altered the ways in which information should be controlled. In addition, it has raised the level of knowledge and skills required to protect an enterprise's information assets, and increased the need for well-educated professionals in the fields of information security, governance of IT and risk management. This need was recognized by the 1969 founding of what is now known as ISACA.

ISACA was formed, and continues to exist today, to meet the unique and diverse technology needs of the continually developing IT field. In an industry in which change is constant, ISACA has moved with agility and speed to bridge the needs of the international business community and the IT control community.

ISACA has become the leading IT governance, assurance, security and control organization. The approximately 95,000 consultants, academics, security professionals, information systems (IS) auditors and senior executives who make up ISACA are spread across 160 countries. ISACA's IT Audit and Assurance and IS Control Standards are followed by practitioners worldwide, and its certifications are recognized globally:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT), designed for professionals who have management, advisory or assurance responsibilities as defined by a "job practice" consisting of IT governance-related tasks and knowledge
- Certified in Risk and Information Systems Control (CRISC), designed for practitioners involved in implementing controls and managing IT and information systems risk

In addition, ISACA publishes the *ISACA Journal*, a leading technical journal in the information control field, and sponsors a series of international conferences focusing on technical and managerial topics. ISACA leads the IT control community and serves its practitioners by providing the elements needed by IT professionals in an ever-changing worldwide environment.

Need for the Model Curriculum for Information Security Management

For a number of years, many employers have been seeking to fill positions with information security professionals who possess a substantial background in security, business and risk management. This demand is expected to grow in the future. Employers have had difficulty in locating a sufficient number of adequately prepared candidates for the available positions. The professionals who do have the requisite background have usually obtained their formal information security education in one of three manners:

- **Participation in a mixture of on-the-job training and in-house programs.** This method of education requires that a professional already be an employee of an enterprise, and it is most appropriate when the technology presented has been adopted and implemented by a

particular enterprise. The on-the-job training and in-house programs are well suited to provide employees with education in a well-defined and limited focus area, but are not well suited to offer a broad-based educational experience for the participants.

- **Participation in workshops/seminars presented by professional enterprises or vendors.** This method is available to professionals from many different enterprises and is valuable in presenting new information or for exploring various approaches to information security problems. In the workshop/seminar environment, a peer group can share perspectives that are not available from a single instructor. However, workshops/seminars are usually more expensive than in-house training, take time away from the office and are typically available only to professionals who are already employed in the workforce. ISACA is well-known for developing and offering high-quality workshops and seminars.
- **Participation in university degree and postgraduate or certificate programs that are delivered within either a full-time or part-time student environment.** These programs can lead to baccalaureate or graduate degrees or to specialized certificates or diplomas. This is the method that can provide professionals (or future professionals) with the most in-depth and broad-based educational experience. Thus, this is the method that ISACA has addressed with its model curriculum efforts.

Typically, students who desire to enter the information security profession, but who lack business experience, seek to gain the required knowledge, skills and abilities through academic/business coursework enhanced by internships. Colleges and universities worldwide are attempting to meet the growing employer demand by educating students and preparing them to enter or to assume a leadership position within the information security profession. At the undergraduate level, some academic institutions have begun to integrate information security courses into their IT and business programs. At the graduate level, some have developed more focused information security programs. Often, however, the academic institutions have relied on existing IT programs to prepare students for the information security profession. Unfortunately, traditional IT programs, by themselves, may be inadequate to meet the needs of both students and employers.

Information security professionals need to be able to cope with the pace of rapid business changes and update themselves regularly with competent knowledge. Recent events, government regulations and changes in business processes have affected the role of information security and the methodologies information security professionals use.

There has been a significant change in responsibilities held by the information security manager. More often, traditional business functions such as compliance, risk management and privacy are being assigned to the information security manager. Therefore, the information security professional must understand not only technological requirements, but also the needs of the business. Therefore, curricula must take into consideration not only the technological challenges, but also the improvement of oral and written communication.

Thus, one of the purposes of a model curriculum for information security is to focus the level of formal education offered by universities. This model is based on the needs and expectations of the information security profession and relies on the prior research of academics, practitioners and professional associations. One objective is to identify the fundamental course components of

information security management so universities can educate students for careers in the information security management field and assist students in becoming marketable in the profession. Although students may not possess actual work experience, the topics identified in the model have been selected to provide graduates with solid skills and capabilities for the profession. The model matches academic offerings with the needs of the profession and provides a framework for academic institutions and professional associations in developing new courses or redesigning their existing course offerings.

ISACA recognizes that each educational institution, whether an accredited college or university, has strengths, weaknesses and constraints that it must address when developing a curriculum. As a result, each educational institution wants to capitalize on its strengths, such as the talent or interests of a particular faculty member, and minimize the effects of its weaknesses (e.g., limited faculty resources to teach particular topics) or constraints (e.g., the number of courses within a degree program that can be devoted to information security topics). Thus, it is unrealistic to expect any institution to cover all of the topics and subtopics to the levels presented in the model. Format, arrangement and content of the proposed curriculum will vary depending on university accreditation and government requirements.

Conclusion

The information security management profession continues to evolve. Universities and other educational institutions must understand the needs of the professional community to provide the market with graduates possessing the required skills and knowledge that enterprises need. The *ISACA Model Curriculum for Information Security Management, 2nd Edition* provides academic institutions with a basic framework of the education required to develop the skills needed to make students employable in the profession.

In the information-based business environment, business professionals who are competent in information security or information security professionals who understand business are in great demand. Information security managers must continually receive training to upgrade their knowledge, skills and abilities. Academic institutions with the appropriate curriculum can generate employable candidates who will be able to assume leadership positions in the information security field. An academic institution that sponsors an information security curriculum that has a business focus is very desirable to those professionals wishing to change their career path or upgrade their skills for job enhancement. The *ISACA Model Curriculum for Information Security Management, 2nd Edition* can be viewed as a reasonably comprehensive set of topics that should be part of an ideal program for information security management. This model curriculum provides a goal for colleges and universities worldwide to strive toward in meeting the demand for educating future information security management professionals.

In addition, the model can serve both those who are interested in obtaining an information security education and educational institutions worldwide that are interested in developing a curriculum in information security.

2. Development

ISACA has long recognized the importance of having model curricula to assist in the development of educational programs for aspiring IT professionals. In 2012, the *ISACA Model Curriculum for Information Systems Audit and Control* was updated to a third edition. With an increased demand for information security professionals with a business focus, the need for a similar update of the 2008 edition of the *ISACA Model Curriculum for Information Security Management* was obvious, especially given the changes to the CISM Review Manual job practices for 2012.

A global committee representing faculty and information security professionals was involved in the development of the first edition of *ISACA Model Curriculum for Information Security Management*, and specialists representing research, standards, education and certification interests reviewed the model. The model is based on the needs and expectations of the information security profession and the prior research of academics, practitioners, audit organizations and professional societies. The model curriculum is considered a living document, to be regularly updated.

The mission statement for the global committee, the Information Security Management Model Curriculum Task Force, was to:

- Create a model curriculum and ensure that it meets the current needs of the information security profession
- Identify course components to fulfill those needs
- Create the specific course descriptions in the model
- Ensure that the model curriculum is in alignment with the most recent *CISM Review Manual*, published by ISACA
- Formulate a plan to stimulate current and future interest in the *ISACA Model Curriculum for Information Security Management* at universities
- Create a procedure for academic institutions to have their programs reviewed by ISACA for model curriculum alignment and, when that alignment is acknowledged, to post that information to the ISACA web site
- Establish a renewal process for reevaluation of college and university programs for alignment with the ISACA model curriculum

It was decided that the best approach to the curriculum development would be to develop a model that presented topical areas to be covered in the program and allow each educational institution or environment to decide the manner in which the educational content would be delivered.

In 2011, a new academic work group was created to revise the first edition.

Creation of the Model

It was agreed that the CISM examination domains could provide a framework for the model curriculum. Thus, the four CISM domains and their subtopics were used to provide a structure to

organize the components of the model curriculum. The four major domains in the CISM examination are:

- Information Security Governance
- Information Risk Management and Compliance
- Information Security Program Development and Management
- Information Security Incident Management

Guidance regarding the amount of educational coverage that should be devoted to each topic area included in the model curriculum needed to be clear enough that users of the model could benefit from the work of the task force, but not so restrictive that faculty members would be constrained in the development or teaching of their courses or in the development of the overall curriculum of a program. The model guidance provides, for each topic, recommended hours of contact time with the students, which is adaptable to the many different educational environments found globally. To develop these contact hour estimates, the task force decided to provide guidance only for the topics within the domain level and not to suggest contact times for every detailed subtopic. With this structure, instructors can decide to devote more time to one or more subtopics within an area and perhaps little or no time to other subtopics.

Discussions with academics and professionals from around the globe indicated that a comprehensive curriculum to train information security management professionals would often include in excess of 300 contact hours. This 300-hour estimate was representative of the time spent in seven, three-credit-hour system courses or about six, five-credit-hour quarter system-based courses. Of course, the 300 hours could be delivered in a variety of formats, including a series of eight-hour education seminars.

The Information Security Management Model Curriculum Task Force and work group understood that institutions would likely have areas that are included in their curricula that might differ from areas included by other institutions. These differences are normal, and the *ISACA Model Curriculum for Information Security Management , 2nd Edition* allows time for teaching these differing topics by identifying topical coverage requiring only 250 hours of contact time (about 80 percent of the 300 hours in many programs). The additional hours in an institution's program can be focused on topics not specifically identified in the model (e.g., topics in Appendix 1. Suggested Supplemental Skills for Information Security Management) or additional coverage of model topics.

An educational institution or professional enterprise can also structure its delivery system components (e.g., courses, modules) to include topics from anywhere within the model and is not limited to any predetermined component structures. To determine alignment with the model, an institution or enterprise should create a mapping of the model curriculum to the topics that are delivered within its educational delivery system components. This mapping could be as simple as providing detailed syllabi of courses taught at a college or university and noting where items from the model curriculum are covered. (An alignment grid can be found in Appendix 2. Alignment Grid.)

Although it is important for the identified topics in the model curriculum to be covered, ISACA recognizes that educational entities have institutional strengths, weaknesses and constraints that

they need to address when developing a curriculum. Format, arrangement and content of the proposed curriculum will vary depending on university accreditation requirements and government requirements. For universities with a business education program in the United States or internationally, use of the Association to Advance Collegiate Schools of Business (AACSB) International, Association of Collegiate Business Schools and Programs (ACBSP), European Quality Improvement System (EQUIS) or Association of MBAs (AMBA) standards is acceptable for curriculum design because the accreditation processes are rigorous and held in high regard by many universities worldwide. Carryover of hours from those areas covered in excess of the recommended number of hours in the model to other areas will be considered by ISACA during the evaluation of the alignment mapping to the model curriculum.

The model curriculum is designed to prepare an individual to pursue a degree with a focus on information security within the scope of a typical program. A typical undergraduate or graduate degree includes programs in business, information security and risk management. The topics in the model curriculum are designed to provide professional skills and capabilities. (See Appendix 1. Suggested Supplemental Skills for Information Security Management.)

3. Use

Alignment with the *ISACA Model Curriculum for Information Security Management, 2nd Edition* entitles the program to be posted on the ISACA web site, and graduates of a compliant program qualify for one year of work experience toward the CISM certification.

The customary methods for delivering education differ greatly throughout the world. Sometimes, universities in some countries do not offer graduate degree programs with established sets of courses as their primary means of advanced education. In some areas, universities offer weekend programs that lead to certificates that are recognized and valued in the professional workplace of those countries.

The *ISACA Model Curriculum for Information Security Management, 2nd Edition* covers topics proposed by a wide range of ISACA members with expertise in information security, IT, governance of IT and risk management. The topics and subtopics selected for inclusion in the model have been deemed important for meeting the knowledge expectations for a recent college graduate seeking to fill a position in the information security management field.

The many topics and subtopics included in the model curriculum are accompanied by contact-hour estimates that provide guidance regarding the amount of educational coverage that should be devoted to each area. These estimates were determined based on the experience and knowledge of the ISACA Model Curriculum Work Group**.** It is envisioned that the contact hours would typically be in some type of classroom, but the model is designed so that the contact could be accomplished through other education delivery methods, including distance learning programs. Thus, if a course meets for concentrated periods of time over a few weekends or meets in a 10-week quarter or 14- to 16-week semester, it should be relatively easy to determine the contact time spent discussing a topic area.

The contact hour guidance is provided only at the topic levels within the domains, not for every detailed subtopic. With this structure, faculty members from any university or educational setting around the world can decide to devote more time to one or more subtopics within a domain and perhaps little or no time to other subtopics. The educational institution could also structure its delivery system components (e.g., courses, modules) to include topics from anywhere within the model and is not limited to any predetermined component structures.

As discussed previously in this document, the topics and subtopics are organized according to the domains for the CISM examination. Detailed descriptions of the topics and subtopics are included in the indicated figures that appear in chapter 4, *ISACA Model Curriculum for Information Security Management, 2nd Edition.*

The **Information Security Governance** domain is divided into nine topic areas, each with one to three different subtopics. The topics cover the subject matter of information security governance as well as the development of information security strategy, architectures and frameworks. Detailed descriptions of the topics and the subtopics are listed in **figure 1**.

The **Information Risk Management** domain is divided into nine topic areas that have from one

to three subtopics each. This domain focuses on the management and assessment of risk in an enterprise, business disaster and recovery planning, and controls and countermeasures. Detailed descriptions of the topics and the subtopics are listed in **figure 2**.

The **Information Security Program Development and Management** domain includes nine topic areas that have from one to two subtopics per area. It includes information regarding the development of a formal security program, including information security program development and management responsibilities; the importance of obtaining senior management's commitment to the program; defining the program; integrating the program into the main organizational business processes; policy development; and the effective management and measurement of an information security program. It also deals with how to implement a security program. Detailed descriptions of the topics and subtopics are listed in **figure 3**.

The **Information Security Incident Management** domain is divided into eight topics with one to two subtopics per topic area. It includes information regarding the definition, establishment and maintenance of an incident management and response process, and organizing and training teams to respond to incidents.

The mapping process steps are detailed in **figure 5** in Appendix 2. Alignment Grid, which provides a form to map an academic program to the model curriculum.

4. *ISACA Model Curriculum for Information Security Management, 2nd Edition*

The topics covered by the model are grouped into four domains. These domains are broken into major topic areas, and subtopics are provided within each topic area, along with the number of contact hours needed to adequately cover the topic. (See **figures 1** through **4**.)

Domain 1. Information Security Governance

Knowledge Objective

Understands the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy and a plan of action to implement it.

Learning Objectives

- Develop an information security strategy aligned with business goals and objectives.
- Align information security strategy with corporate governance.
- Develop business cases justifying investment in information security.
- Identify current and potential legal and regulatory requirements.
- Identify drivers affecting the enterprise.
- Obtain senior management commitment.
- Define roles and responsibilities for information security.
- Establish internal and external reporting and communication channels.

Figure 1—Information Security Governance Domain

Topic	Hours	Subtopic
Establish an information security strategy in alignment with organizational goals to guide the establishment of an information security program.	**5**	Developing an information security strategy
		Understanding the relationship among information security and business goals, objectives, functions and practices
		Developing strategic plans that include resourcing (personnel, third parties) and constraints (regulatory, culture, costs)
Establish and maintain an information security governance framework.	**7**	Methods to implement an information security governance framework. These should include the following concepts: • Purpose and outcomes of governance • Relationship of governance to strategy and controls • The relationship of security governance to enterprise governance • How governance is implemented
		Understanding internationally recognized standards, frameworks and best practices related to information security and strategy development. (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 27002, National Institute of Standards and Technology [NIST] 53, COBIT, Enterprise Information Security Architecture [EISA]). The concepts should include: • Purpose of standards • When and how standards are used • The attributes of international standards • The relationship to ISO and COBIT

Figure 1—Information Security Governance Domain		
Topic	**Hours**	**Subtopic**
Integration of information security governance into enterprise governance to ensure that organizational goals and objectives are supported by the information security program.	**4**	The fundamental concepts of governance and how they relate to information security. The concepts should include, but are not limited to: • Security linkages to organizational functions • Organizational benefits of effective security • Determining the effectiveness of information security governance
		Integrating information security governance into corporate governance. The concepts should include, but are not limited to: • Methods to determine acceptable risk • Approaches to developing risk mitigating strategies
Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.	**6**	The development of information security policies. The concepts should include, but are not limited to: • The basis for policy development • The differences between policies, standards and procedures • Policy and strategy
Develop business cases to support investments in information security.	**5**	Business case methods. The concepts should include, but are not limited to: • The purpose of a business case • What is included in a business case • Business benefits and impact analysis • Financial aspects of a business case
		Strategic budget planning and reporting methods. The concepts should include, but are not limited to: • Budgeting • Financial reporting
Identify internal and external influences to the enterprise (e.g., technology, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by information security strategy.	**8**	Internal and external influences (e.g., regulatory compliance: Health Insurance Portability and Accountability Act [HIPAA], Health Information Technology for Economic and Clinical Health [HITECH] 2009 Act, Payment Card Industry Data Security Standard [PCI DSS], Federal Trade Commission [FTC], Gramm-Leach-Bliley Act [GLBA], Sarbanes-Oxley Act). The concepts should include, but are not limited to: • Cultural aspects of organizational reactions and responses • Regulatory drivers and impacts • Business sector differences
Obtain senior management commitment and support from stakeholders to maximize the successful implementation of information security.	**5**	Communication methods to obtain commitment and support. The concepts should include, but are not limited to: • The effects of inadequate managements support • Risk tolerance • How to achieve management commitment to information security
		Organizational structures and lines of authority. The concepts should include, but are not limited to: • Organizational structure and governance • Responsibilities and segregation of duties
Define and communicate roles and responsibilities to establish clear accountabilities.	**4**	Information security management roles and responsibilities and how to develop segregation of duty profiles. The concepts should include, but are not limited to: • Variation in roles and responsibilities of information

Figure 1—Information Security Governance Domain		
Topic	**Hours**	**Subtopic**
		security • The impact of organizational structure on information security management • Impact of other influences on the roles and responsibilities of information security management
Establish, monitor, evaluate and report metrics (key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of information security strategy.	**6**	Methods of selecting and implementing key metrics. The concepts should include, but are not limited to: • Strategic and management metrics (the differences) • KGIs • KPIs • KRIs
		Methods to establish reporting and communicating channels throughout the enterprise. The concepts should include, but are not limited to: • Types of security events to be communicated • Types of information and how to report it • Integrating other assurance processes with information security
Total	**50**	

Domain 2. Information Risk Management and Compliance

Knowledge Objective

Understands the importance of risk management as a tool for meeting business needs and developing a security management program to support these needs while managing information risk to an acceptable level to meet the business and compliance requirements of the organization

Learning Objectives

- Establish a process for information asset classification and ownership.
- Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- Implement a systematic 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 evaluate information security controls and countermeasures.
- Integrate risk, threat and vulnerability identification and management into life cycle processes.
- Identify the gap between current and desired risk levels to manage risk to an acceptable level.
- Integrate information risk management into business and IT processes (for example, development, procurement, project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the enterprise.
- Report significant changes in information risk to appropriate levels of management.

Figure 2—Information Risk Management and Compliance Domain		
Topic	**Hours**	**Subtopic**
Establish and maintain a process for information asset classification to ensure that measures taken to protect assets are in proportion to their business value.	**5**	Data classification models. The concepts should include, but are not limited to: • The purpose of asset classification • Determining the basis for classifications

Figure 2—Information Risk Management and Compliance Domain		
Topic	**Hours**	**Subtopic**
		• The relationship to business continuity planning (BCP) and disaster recovery planning (DRP) • Determining sensitivity and criticality • Relationship between, risk, impact, sensitivity and criticality
		Information asset valuation methodologies. The concepts should include, but are not limited to: • Purpose and benefits of asset valuation • The relationship of valuation and impact assessment • Methodology methods such as risk assessment, information resource valuation
Identify legal, regulatory, organizational and other applicable requirements to manage risk of noncompliance to acceptable levels.	**5**	Control legal and regulatory considerations in a risk management strategy
		Operational compliance risk
		Legal and regulatory considerations for asset classifications
Ensure that risk assessments, vulnerability and threat analysis are conducted periodically and consistently to identify risk to the enterprise's information.	**7**	Threat and vulnerability analysis methods
		Risk events that affect risk assessments
		Risk assessment and analysis methodologies
Determine appropriate risk response options to manage risk to acceptable levels.	**5**	Risk prioritization methods
		Risk response techniques
Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.	**8**	Control baseline modeling and its relationship to risk-based assessments. The concepts should include, but are not limited to: • Risk management issues related to life cycles • Information life cycles • Change management and life cycles
		Information security controls and countermeasures and the methods to analyze their effectiveness
Perform a gap analysis. Identify current and desired risk levels to manage risk to acceptable levels.	**5**	Gap analysis techniques. The concepts should include, but are not limited to: • Controls and control objectives that affect information security • Determining current state and desired or target state • Determining the current risk posture
Integrate information security risk management into the enterprise risk management (ERM) process, including other IT processes (e.g., project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the enterprise.	**5**	Organizational or ERM methodologies and the techniques for integrating information security risk management into them
Monitor risk to ensure that changes are identified and managed appropriately.	**5**	Risk monitoring techniques and how they integrate with incident management techniques. The concepts should include, but are not limited to: • Monitoring key controls • Consideration of physical and technical monitoring techniques • Monitoring approaches (what should be monitored)

Figure 2—Information Risk Management and Compliance Domain		
Topic	**Hours**	**Subtopic**
Report risk to assist in the decision-making process of the organization.	**5**	Risk reporting requirements (e.g., frequency, adequacy, audience)
		Compliance reporting requirements. Taking into consideration risk management issues related to change management and life cycles.
Total	**50**	

Domain 3. Information Security Program Development and Management

Knowledge Objective

Understands the broad requirements and activities needed to create, manage and maintain a program to implement an information security strategy. The information security program may consist of a series of projects and initiatives to achieve the objectives the strategy is designed to address as well as ongoing management and administration.

Learning Objectives

- 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.
- Identify and manage internal and external resources required to execute the information security program.
- Ensure the development of information security architectures.
- Establish and ensure the development, communication and maintenance of standards, procedures and other documentation that support information security policies.
- Design and develop a program for information security awareness, training and education to stakeholders.
- Provide information security advice and guidance in the enterprise.
- Monitor, measure, test and report on the effectiveness and efficiency of information security controls and compliance with information security policies.
- Ensure that processes and procedures are performed in compliance with the organization's information security policies and standards.
- Ensure and integrate information security requirements into the organization's processes and life cycle activities.
- Develop a process to integrate information security controls into contracts.
- Ensure the performance of contractually agreed information security controls.
- Ensure that information security is an integral part of the systems development process and acquisition processes.
- Ensure that noncompliance issues and other variances are resolved in a timely manner.
- Establish metrics to evaluate the effectiveness of the information security program.

Figure 3—Information Security Program Development and Management Domain		
Topic	**Hours**	**Subtopic**
Establish and maintain an information security program.	**10**	Information security architectures (e.g., people, processes, technology) and methods to apply them. The concepts should include, but are not limited to: • Purpose of security architecture

Figure 3—Information Security Program Development and Management Domain		
Topic	**Hours**	**Subtopic**
		• The elements of a security architecture • Types of security architecture
Align the information security program to other business functions (e.g., accounting, procurement) to support business process integration.	**10**	Methods to align information security program requirements with those of other business functions. The concepts should include, but are not limited to: • Functions of other organizational units related to information security • Factors affecting interdepartmental collaboration • Structural and cultural considerations for alignment • Integration of policy, governance and process
Identify, acquire, manage and define internal and external resources to execute the information security program.	**15**	Identify, acquire, manage and define requirements for internal and external resources. The concepts should include, but are not limited to: • Effective project planning and management • Resources required for information security program implementation • Security requirements for outsourced functions and services • Risks and liabilities posed by third parties
Establish and maintain information security architectures (people, process, technologies) to execute the information security program.	**10**	Information security technologies and underlying concepts and trends (e.g., cloud computing, mobile computing). The concepts should include, but are not limited to: • Types of security technologies • Use and purpose of security technologies • Control technologies • Security information technology
Establish and maintain a program for organizational standards, procedures, guidelines and documentation to support and guide compliance with information security policies.	**15**	Information security standards, procedures and guidelines. The concepts should include, but are not limited to: • Circumstances requiring control documentation changes • Implementation of policies and standards • Requirements for evaluating control documentation
		Methods to implement and communicate information security policies, standards, procedures and guidelines
Establish and maintain a program for security awareness and training to promote a secure environment and effective security culture.	**10**	Information security awareness and training programs. This should include determining adequate levels of security awareness.
Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, development, BCP, and DRP) to maintain the enterprise's security baseline.	**15**	Integrating information security requirements into organizational processes (taking into consideration the outcomes for information security program management, and outsourcing and service providers).
		The design information security controls. The concepts should include, but are not limited to: • The kinds of controls and their uses • Control design criteria • Control design policy • Control testing and maintenance • Control development, performance and deployment criteria

Figure 3—Information Security Program Development and Management Domain		
Topic	**Hours**	**Subtopic**
Integrate the information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, customers) to maintain the enterprise's security baseline.	**10**	Methods to incorporate information security requirements into contracts and third-party management processes. The concepts should include, but are not limited to: • The types and degree of information security risk posed by contractual relationships • Liabilities posed by third parties • Contract and relationship monitoring and metrics
Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.	**10**	Testing the effectiveness and applicability of information security controls. The concepts should include, but are not limited to: • Purpose of testing • Methods of testing controls • Control testing criteria • Legal and regulatory control testing requirements
		Operational information security metrics. The concepts should include, but are not limited to: • Types of strategic management and operational metrics • Purpose and use of metrics • Essential criteria for relevant metrics • What should be monitored
Total	**105**	

Domain 4. Information Security Incident Management

Knowledge Objective

Possess the knowledge and understanding necessary to identify, analyze, manage and respond effectively to unexpected events that may adversely affect the enterprise's information assets and/or its ability to operate.

Learning Objectives

- Develop and implement processes for 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.
- Develop a process to communicate with internal parties and external organizations.
- Integrate information security incident response plans with the enterprise's DRP and BCP.
- 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.
- Establish and maintain integration among the incident response plan, DRP and BCP.

Figure 4—Information Security Incident Management Domain		
Topic	**Hours**	**Subtopic**
Establish, define and maintain an organizational definition of information security incidents to allow accurate identification of and response to incidents.	**5**	Incident classification methods. The concepts should include, but are not limited to: • Incident classification • Severity levels • Action plans for incident response
		The components of an incident response plan. The concepts should include, but are not limited to: • Incident response team responsibilities • How to identify an incident • Incident triage (process of sorting, categorizing, correlating, prioritizing and assigning incoming reports/events)
Develop and implement processes to ensure the timely identification of incidents.	**7**	Incident management concepts and practices. The concepts should include, but are not limited to: • Incident management life cycle • Incident management processes • Incident response capabilities • Incident management response purpose
Establish and maintain processes to investigate and document incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organized requirements.	**7**	Forensics requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality, chain of custody, completeness of evidence). The concepts should include, but are not limited to: • Collection and preservation of evidence • Chain of custody • Investigating techniques
		Types and sources of tools and equipment required to adequately equip incident response teams. This should include investigative tools and the response team capability requirements.
Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.	**7**	Technologies and processes that detect log and analyze information security events. This should include intrusion detection systems (IDSs), intrusion prevention systems (IPSs), host-based intrusion detection systems (HIDSs) and network intrusion detection systems (NIDSs).
		Damage containment methods. The concepts should include, but are not limited to: • How to contain an incident • Problem management • Response capability itself
Organize, train and equip teams to respond to incidents.	**5**	Roles and responsibilities in identifying and managing information security incidents. The concepts should include, but are not limited to: • Event, incident and problem definitions • Types of roles and corresponding responsibilities • Skills and personnel requirements • Evidence collection and handling
		Techniques to quantify damages, costs and other business impacts arising from information security incidents. The concepts should include, but are not limited to: • Financial impact assessments and analysis • Techniques for quantifying financial impacts • Third-party liability and exposures

Figure 4—Information Security Incident Management Domain		
Topic	**Hours**	**Subtopic**
Establish and maintain communication plans and processes to manage communication with internal and external entities (including the government), including the testing and reviewing of the incident response plan.	**5**	Notification and escalation processes. The concepts should include, but are not limited to: • Severity criteria • Communication and reporting channels • Escalation procedures
		Internal and external incident reporting requirements and procedures, taking into consideration legal and regulatory reporting requirements
Postincident reviews	**4**	Postincidental review practices and investigating methods to identify root causes to determine corrective actions. The concepts should include, but are not limited to: • Postmortem assessments, analysis and reporting • Problem management and root cause analysis • Forensics
Establish and maintain integration between BCP/DRP and crisis management systems in the enterprise.	**5**	BCP, DRP, crisis management and their relationship to the incident response plan. The concepts should include, but are not limited to: • BCP techniques • DRP techniques • An understanding of acceptable service levels • The execution of response and recovery plans
Total	**45**	
Grand Total	**250**	**Total hours for domains 1 through 4**

Appendix 1. Suggested Supplemental Skills for Information Security Management

The following competencies are not required components to the *ISACA Model Curriculum for Information Security Management, 2nd Edition*, but they are important skills for information security managers.

IT Security—Skills that are technical in nature and may include topics such as penetration testing, continuous monitoring and security architecture

Enterprise Risk Management (ERM)—Topics to be discussed may include organizational risk and the convergence of physical and information security.

Regulation, Standards and Frameworks—Topics to be covered may include international and regional legislation, such as the US Sarbanes-Oxley Act, Japan's Financial Instruments and Exchange Law (J-SOX), GLBA, HIPAA, the HITECH Act, the US Federal Rules of Civil Procedure, the European Union's Data Protection Directive, ISO/IEC 27001/27002, NIST, PCI DSS, COBIT, etc.

Managerial Communications and/or Public Speaking—Includes communication skills that are employed when discussing security program metrics and program recommendations

Interviewing Skills—Includes the effective gathering of information when interviewing management and completing control questionnaires

Negotiation Skills and/or Personal Selling—Includes skills needed to convince management to implement recommendations for positive change

Business Writing—Includes skills useful to produce understandable and usable reports and other written communications

Industrial Psychology and/or Behavioral Science—Includes the ability to understand and effectively manage human behavior and organizational culture to maximize the security program success

Project Management/Time Budgeting—Includes the essential ability to effectively and efficiently manage time and tasks

Team Building and Team Leading—Includes effectively managing team activities with proper coordination and utilization of knowledge and skills of individual team members for information security

Appendix 2. Alignment Grid

To map a program to the *ISACA Model Curriculum for Information Security Management, 2nd Edition*, enter the name of the course(s) or session(s) in the program that covers each topic area or subtopic description along with the amount of time (in whole hours) devoted to covering the topic in each table. If a described topic is not covered, record a 0 (zero) in the column for contact hours. To be in alignment with the model, the total time spent, in hours, should be at least 250 hours, and all areas in the model curriculum should have reasonable coverage. Up to a maximum of 25 noncontact hours may be included. When mapping a graduate program, include the prerequisites from the undergraduate program.

Before beginning this process:

- Obtain the current course syllabi. Current, expanded course outlines provide more detail and are better sources.
- Ensure that the current textbook supporting the classes and the visual media/projects used in those classes are accessible. For a question on content, refer to the course textbook or PowerPoint® slides.
- If some of the subject matter is taught in other departments or colleges, a representative who is knowledgeable of the content of those classes may need to provide assistance. For this reason, an undergraduate program may take more time to map than a graduate program.

A dual monitor, with the model matrix on one screen and the syllabus/expanded course outline on the other, facilitates the process.

The mapping process steps are listed in **figure 5**.

Figure 5—Mapping Process Steps	
1	Identify all direct and support courses that apply to the program. Course syllabi are to contain at least the following information: school name and address, course title, course number, contact hours, faculty member names and credentials, terms offered, the purpose of the course, the objectives of the course, and the course text.
2	Ensure that the current syllabi or expanded course outlines and support materials for the courses are accessible. It takes approximately 16 hours to complete the mapping, if expanded course outlines are available from which information can be extracted.
3	Proceed one by one. Select the first course in the program, examine the elements and subject matter, and map to the model. Proceed week by week.
4	Use key words from the ISACA template subtopics to search the syllabi to identify matches. Once a match is made, estimate the amount of time devoted to the subject based on the syllabus.
5	If uncertain of the content of the subject covered, go to the textbook and PowerPoint slides/materials used. Note that generic titles used often cover more than what is implied.
6	Remember to allocate the time per course and identify the course covering each subject. For example, a quarter system may have 10 weeks and four contact hours per week (40 hours), but some courses may have lab or project requirements that may result in more than 40 hours.
7	Map course by course and keep track of allocation. This is easiest for those familiar with the program and who have the information available.
8	After completing all courses, go back and double-check that the selections/placement are the best possible and seem reasonable.
9	Have a colleague check the mapping.
10	Submit the completed tables to ISACA for review by email to *research@isaca.org*, fax to +1.847.253.1443, or mail to the attention of the Manager of Information Security Practices, ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA.

If the program is found to be in alignment with the *ISACA Model Curriculum for Information Security Management, 2nd Edition*, the program may be posted on the ISACA web site and graduates of the program will qualify for one year of work experience toward the CISM certification. The following pages include domains 1 through 4 with blank columns added for the course and number of hours, which institutions can use to map their programs to the model curriculum.

Domain 1—Information Security Governance				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Establish an information security strategy in alignment with organizational goals to guide the establishment of an information security program.	**5**	Developing an information security strategy		
		Understanding the relationship among information security and business goals, objectives, functions and practices		
		Developing strategic plans that include resourcing (personnel, third parties) and constraints (regulatory, culture, costs)		
Establish and maintain an information security governance framework.	**7**	Methods to implement an information security governance framework. These should include the following concepts: • Purpose and outcomes of governance • Relationship of governance to strategy and controls • The relationship of security governance to enterprise governance • How governance is implemented		
		Understanding internationally recognized standards, frameworks and best practices related to information security and strategy development. (e.g., International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 27002, National Institute of Standards and Technology [NIST] 53, COBIT, Enterprise Information Security Architecture [EISA]). The concepts should include: • Purpose of standards • When and how standards are used • The attributes of international standards • The relationship to ISO and COBIT		
Integration of information security governance into enterprise governance to ensure that organizational goals and objectives are supported by the information security program.	**4**	The fundamental concepts of governance and how they relate to information security. The concepts should include, but are not limited to: • Security linkages to organizational functions • Organizational benefits of effective security • Determining the effectiveness of information security governance		
		Integrating information security governance into corporate governance. The concepts should include, but are not limited to:		

Domain 1—Information Security Governance				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
		• Methods to determine acceptable risk • Approaches to developing risk mitigating strategies		
Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures and guidelines.	**6**	The development of information security policies. The concepts should include, but are not limited to: • The basis for policy development • The differences between policies, standards and procedures • Policy and strategy		
Develop business cases to support investments in information security.	**5**	Business case methods. The concepts should include, but are not limited to: • The purpose of a business case • What is included in a business case • Business benefits and impact analysis • Financial aspects of a business case		
		Strategic budget planning and reporting methods. The concepts should include, but are not limited to: • Budgeting • Financial reporting		
Identify internal and external influences to the enterprise (e.g., technology, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by information security strategy.	**8**	Internal and external influences (e.g., regulatory compliance: Health Insurance Portability and Accountability Act [HIPAA], Health Information Technology for Economic and Clinical Health [HITECH] 2009 Act, Payment Card Industry Data Security Standard [PCI DSS], Federal Trade Commission [FTC], Gramm-Leach-Bliley Act [GLBA], Sarbanes-Oxley Act). The concepts should include, but are not limited to: • Cultural aspects of organizational reactions and responses • Regulatory drivers and impacts • Business sector differences		
Obtain senior management commitment and support from stakeholders to maximize the successful implementation of information security.	**5**	Communication methods to obtain commitment and support. The concepts should include, but are not limited to: • The effects of inadequate managements support • Risk tolerance • How to achieve management commitment to information security		
		Organizational structures and lines of authority. The concepts should include, but are not limited to: • Organizational structure and governance • Responsibilities and segregation of duties		

Domain 1—Information Security Governance				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Define and communicate roles and responsibilities to establish clear accountabilities.	**4**	Information security management roles and responsibilities and how to develop segregation of duty profiles. The concepts should include, but are not limited to: • Variation in roles and responsibilities of information security • The impact of organizational structure on information security management • Impact of other influences on the roles and responsibilities of information security management		
Establish, monitor, evaluate and report metrics (key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of information security strategy.	**6**	Methods of selecting and implementing key metrics. The concepts should include, but are not limited to: • Strategic and management metrics (the differences) • KGIs • KPIs • KRIs		
		Methods to establish reporting and communicating channels throughout the enterprise. The concepts should include, but are not limited to: • Types of security events to be communicated • Types of information and how to report it • Integrating other assurance processes with information security		
Total	**50**			

Domain 2—Information Risk Management and Compliance				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Establish and maintain a process for information asset classification to ensure that measures taken to protect assets are in proportion to their business value.	**5**	Data classification models. The concepts should include, but are not limited to: • The purpose of asset classification • Determining the basis for classifications • The relationship to BCP and DRP • Determining sensitivity and criticality • Relationship between, risk, impact, sensitivity and criticality		
		Information asset valuation methodologies. The concepts should include, but are not limited to: • Purpose and benefits of asset valuation • The relationship of valuation and impact assessment • Methodology methods such as risk assessment, information resource valuation		
Identify legal, regulatory, organizational and other applicable requirements to manage risk of noncompliance to acceptable levels.	**5**	Control legal and regulatory considerations in a risk management strategy		
		Operational compliance risk		
		Legal and regulatory considerations for asset classifications		
Ensure that risk assessments, vulnerability and threat analysis are conducted periodically and consistently to identify risk to the enterprise's information.	**7**	Threat and vulnerability analysis methods		
		Risk events that affect risk assessments		
		Risk assessment and analysis methodologies		
Determine appropriate risk response options to manage risk to acceptable levels.	**5**	Risk prioritization methods		
		Risk response techniques		
Evaluate information security controls to determine whether they are appropriate and effectively mitigate risk to an acceptable level.	**8**	Control baseline modeling and its relationship to risk-based assessments. The concepts should include, but are not limited to: • Risk management issues related to life cycles • Information life cycles • Change management and life cycles		
		Information security controls and countermeasures and the methods to analyze their effectiveness		
Perform a gap analysis. Identify current and desired risk levels to manage risk to acceptable levels.	**5**	Gap analysis techniques. The concepts should include, but are not limited to: • Controls and control objectives that affect information security • Determining current state and desired or target state • Determining the current risk posture		

Domain 2—Information Risk Management and Compliance				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Integrate information security risk management into the enterprise risk management (ERM) process, including other IT processes (e.g., project management, mergers and acquisitions) to promote a consistent and comprehensive information risk management process across the enterprise.	**5**	Organizational or ERM methodologies and the techniques for integrating information security risk management into them		
Monitor risk to ensure that changes are identified and managed appropriately.	**5**	Risk monitoring techniques and how they integrate with incident management techniques. The concepts should include, but are not limited to: • Monitoring key controls • Consideration of physical and technical monitoring techniques • Monitoring approaches (what should be monitored)		
Report risk to assist in the decision-making process of the organization.	**5**	Risk reporting requirements (e.g., frequency, adequacy, audience)		
		Compliance reporting requirements. Taking into consideration risk management issues related to change management and life cycles.		
Total	**50**			

Domain 3—Information Security Program Development and Management				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Establish and maintain an information security program.	**10**	Information security architectures (e.g., people, processes, technology) and methods to apply them. The concepts should include, but are not limited to: • Purpose of security architecture • The elements of a security architecture • Types of security architecture		
Align the information security program to other business functions (e.g., accounting, procurement) to support business process integration.	**10**	Methods to align information security program requirements with those of other business functions. The concepts should include, but are not limited to: • Functions of other organizational units related to information security • Factors affecting interdepartmental collaboration • Structural and cultural considerations for alignment • Integration of policy, governance and process		
Identify, acquire, manage and define internal and external resources to execute the information security program.	**15**	Identify, acquire, manage and define requirements for internal and external resources. The concepts should include, but are not limited to: • Effective project planning and management • Resources required for information security program implementation • Security requirements for outsourced functions and services • Risks and liabilities posed by third parties		
Establish and maintain information security architectures (people, process, technologies) to execute the information security program.	**10**	Information security technologies and underlying concepts and trends (e.g., cloud computing, mobile computing). The concepts should include, but are not limited to: • Types of security technologies • Use and purpose of security technologies • Control technologies • Security information technology		
Establish and maintain a program for organizational standards, procedures, guidelines and documentation to support and guide compliance with information security policies.	**15**	Information security standards, procedures and guidelines. The concepts should include, but are not limited to: • Circumstances requiring control documentation changes • Implementation of policies and standards • Requirements for evaluating control documentation		
		Methods to implement and communicate information security policies, standards, procedures and guidelines		

Domain 3—Information Security Program Development and Management				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Establish and maintain a program for security awareness and training to promote a secure environment and effective security culture.	**10**	Information security awareness and training programs. This should include determining adequate levels of security awareness.		
Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, development, BCP, and DRP) to maintain the enterprise's security baseline.	**15**	Integrating information security requirements into organizational processes (taking into consideration the outcomes for information security program management, and outsourcing and service providers).		
		The design information security controls. The concepts should include, but are not limited to: • The kinds of controls and their uses • Control design criteria • Control design policy • Control testing and maintenance • Control development, performance and deployment criteria		
Integrate the information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, customers) to maintain the enterprise's security baseline.	**10**	Methods to incorporate information security requirements into contracts and third-party management processes. The concepts should include, but are not limited to: • The types and degree of information security risk posed by contractual relationships • Liabilities posed by third parties • Contract and relationship monitoring and metrics		
Establish, monitor and periodically report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.	**10**	Testing the effectiveness and applicability of information security controls. The concepts should include, but are not limited to: • Purpose of testing • Methods of testing controls • Control testing criteria • Legal and regulatory control testing requirements		
		Operational information security metrics. The concepts should include, but are not limited to: • Types of strategic management and operational metrics • Purpose and use of metrics • Essential criteria for relevant metrics • What should be monitored		
Total	**105**			

Domain 4—Information Security Incident Management				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
Establish, define and maintain an organizational definition of information security incidents to allow accurate identification of and response to incidents.	**5**	Incident classification methods. The concepts should include, but are not limited to: • Incident classification • Severity levels • Action plans for incident response		
		The components of an incident response plan. The concepts should include, but are not limited to: • Incident response team responsibilities • How to identify an incident • Incident triage (process of sorting, categorizing, correlating, prioritizing and assigning incoming reports/events)		
Develop and implement processes to ensure the timely identification of incidents.	**7**	Incident management concepts and practices. The concepts should include, but are not limited to: • Incident management life cycle • Incident management processes • Incident response capabilities • Incident management response purpose		
Establish and maintain processes to investigate and document incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organized requirements.	**7**	Forensics requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality, chain of custody, completeness of evidence). The concepts should include, but are not limited to: • Collection and preservation of evidence • Chain of custody • Investigating techniques		
		Types and sources of tools and equipment required to adequately equip incident response teams. This should include investigative tools and the response team capability requirements.		
Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.	**7**	Technologies and processes that detect log and analyze information security events. This should include IDSs, IPSs, HIDSs and NIDSs.		
		Damage containment methods. The concepts should include, but are not limited to: • How to contain an incident • Problem management • Response capability itself		
Organize, train and equip teams to respond to incidents.	**5**	Roles and responsibilities in identifying and managing information security incidents. The concepts should include, but are not limited to: • Event, incident and problem definitions • Types of roles and corresponding responsibilities		

Domain 4—Information Security Incident Management				
Topic	**Hours**	**Subtopic**	**Course(s) covering the subtopic**	**Hours**
		• Skills and personnel requirements • Evidence collection and handling		
		Techniques to quantify damages, costs and other business impacts arising from information security incidents. The concepts should include, but are not limited to: • Financial impact assessments and analysis • Techniques for quantifying financial impacts • Third-party liability and exposures		
Establish and maintain communication plans and processes to manage communication with internal and external entities (including the government), including the testing and reviewing of the incident response plan.	**5**	Notification and escalation processes. The concepts should include, but are not limited to: • Severity criteria • Communication and reporting channels • Escalation procedure		
		Internal and external incident reporting requirements and procedures, taking into consideration legal and regulatory reporting requirements		
Postincident reviews	**4**	Postincident review practices and investigating methods to identify root causes to determine corrective actions. The concepts should include, but are not limited to: • Postmortem assessments, analysis and reporting • Problem management and root cause analysis • Forensics		
Establish and maintain integration between BCP/DRP and crisis management systems in the enterprise.	**5**	BCP, DRP, crisis management and their relationship to the incident response plan. The concepts should include, but are not limited to: • DRP techniques • BCP techniques • An understanding of acceptable service levels • The execution of response and recovery plans		
Total	**45**			

Grand Total	**250**	**Total hours for domains 1 through 4**		

Appendix 3. References

ISACA, CISM Job Practice Areas, 2012, *www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/Job-Practice-Areas/Pages/default.aspx*

ISACA, COBIT® 4.1, USA, 2007, *www.isaca.org/cobit*

ISACA, *ISACA® Model Curriculum for Information Systems Audit and Control, 3rd Edition*, USA, 2012

