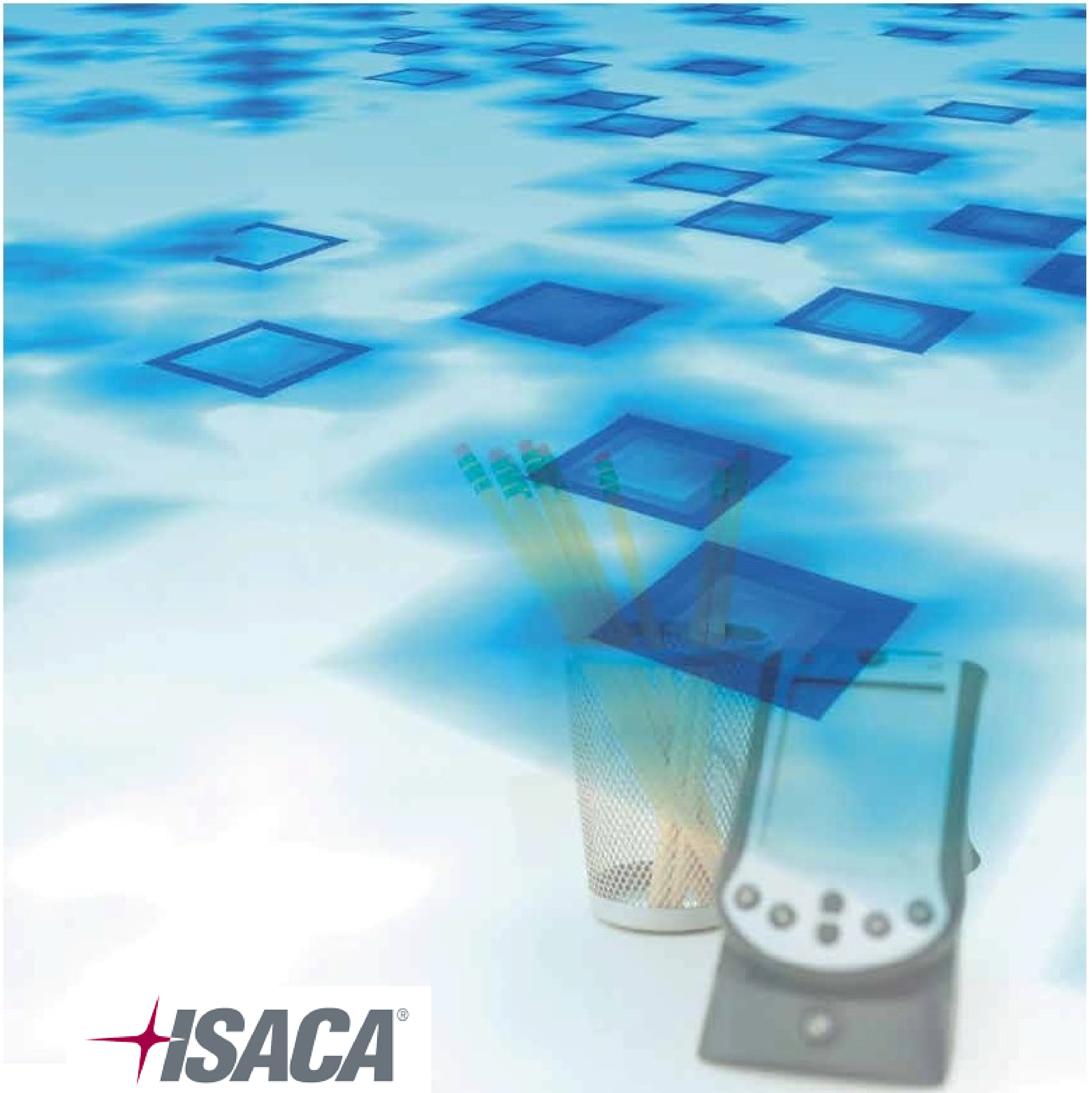


Trust in, and value from, information systems

ISACA® Model Curriculum for IS Audit and Control, 3rd 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 IS Audit and Control, 3rd Edition* (the “Work”), primarily as an educational resource for academics, assurance and control 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, audit professionals should apply their own professional judgment to the specific control 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*

ISACA Model Curriculum for IS Audit and Control, 3rd 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, CFE, CBCP, Ernst & Young LLP, Singapore
Phil Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, 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
ASI System Integration
Hewlett-Packard
IBM
SOAProjects Inc.
Symantec Corp.
TruArx Inc.

Table of Contents

1. Background

ISACA History

The evolution of information technology (IT) continues to significantly affect the business environment. It changes business practices, reduces costs and alters the ways in which systems should be controlled. In addition, it raises the level of knowledge and skills required to control and audit information systems, and it increases the need for well-educated professionals in the fields of information systems (IS) governance, assurance, security and control. This need was recognized in 1969 by the association 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, 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 internal 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 an Updated Model Curriculum

ISACA revised the original *ISACA Model Curriculum for IS Audit and Control* in 2004 and early 2009 to respond to the increasing market need for accounting and assurance professionals with substantial background in audit, control and IT. Since 2009, ISACA has updated its job practices in the CISA certification, which required a full update of the model curriculum. The need to fill positions with adequately prepared candidates continues to exist, and many professionals who have the requisite background obtain their IS auditing education through a university degree or certificate programs, which 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 IS audit and control profession, but who lack business experience, seek to gain the required knowledge, skills and abilities through academic/business coursework enhanced by internships. Worldwide, universities are attempting to meet the growing employer demand by educating students for the IS audit profession. At the undergraduate level, some universities have begun to integrate IS courses into their accounting and business programs and accounting and business courses into their IS programs. At the graduate level, some have developed more focused IS assurance programs. Often, however, the universities have relied on existing accounting or information systems programs to prepare students for the IS audit and control profession. Unfortunately, traditional accounting or IS programs by themselves may be inadequate to meet the needs of employers. The historical—and currently most common—approach for this education is for students to take a set of core business courses and selected courses in one specialization (e.g., accounting, information systems or computer science) and then perhaps one or two courses in a second area, such as information systems or accounting, usually without coordination of course content among the various disciplines.

IS auditors need to be able to cope with the rapid pace of technological change and regularly update their technical knowledge. Recent events, government regulations and changes in business processes have affected the role of IS audit and the methodologies that IS auditors use. Therefore, the IS audit professional must understand the new technologies, be capable of determining their impact on the control process and audit procedures, and clearly communicate that evidence collection tools and techniques have been developed. The curriculum must not only take into consideration the technological challenges, but also the issues involving improvement of oral and written communication abilities.

Thus, one of the purposes of a model curriculum for IS audit and control is to focus the level of formal education offered by universities. This model is based on the needs and expectations of the IS audit and control profession and relies on the prior research of academics, practitioners, audit organizations and professional associations. One objective is to identify the fundamental course components of IS audit and control so that universities can educate students for careers in the IS audit and assurance profession and assist students in becoming marketable in the field. Although students may not possess actual work experience, the topics identified in the model have been selected to provide graduates with entry-level skills and capabilities for the profession. The model matches academic offerings with the needs of the profession and provides a framework for universities and professional associations in developing new courses or redesigning their existing course offerings.

ISACA recognizes that each educational institution, whether a university or other professional organization, has institutional strengths, weaknesses and constraints that it must address when developing a curriculum. As a result, each educational organization wants to capitalize on its strengths (e.g., 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 IS audit and control topics). Thus, it is unrealistic to expect any institution to cover all of the topics and subtopics to the levels presented in the model. 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. Format, arrangement and content of the proposed curriculum will vary depending on university accreditation and government requirements.

Note that, in 2008, ISACA also issued *ISACA Model Curriculum for Information Security Management*, and this also is being updated. This reasonably comprehensive set of topics should be part of an ideal program for information security management. It provides a goal for colleges and universities worldwide to strive toward in meeting the demand for educating future information security management professionals.

Conclusion

The IS audit and control profession continues to evolve. ISACA's COBIT 4.1 is an example of the IT control objectives confronting management, auditors, IS professionals and users. Universities and other educational institutions must understand the needs of the professional community to provide the market with graduates possessing the skills and knowledge that the profession needs. The *ISACA Model Curriculum for IS Audit and Control, 3rd Edition* provides universities with a streamlined approach for providing the education required to develop the skills needed to be employable in the IS audit and assurance profession.

In the information-based business environment, professionals who are technically competent in IS, or IS specialists who understand accounting, commerce and financial operations, are in great demand for IS audit careers. The IS specialist and the IS auditor must continually receive training to upgrade their knowledge, skills and abilities. Universities with the appropriate curriculum can generate employable candidates for the IS audit and control profession. A proactive university that sponsors an IS audit and control curriculum is very desirable to those professionals wishing to change their career path or upgrade their skills for job enhancement. The *ISACA Model Curriculum for IS Audit and Control, 3rd Edition*, is a reasonably comprehensive set of topics for an ideal program for IS audit and control. It provides a goal for universities worldwide to strive toward in meeting the demand for educating future IS professionals.

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

2. Development

ISACA has long recognized the importance of having a model curriculum to assist in the development of programs for aspiring IS assurance professionals, and released the first model curriculum in March 1998. A global committee representing faculty from 15 undergraduate and graduate schools and practitioners from 20 companies was involved in the development of the model, and other ISACA specialists representing research, standards, education and certification interests reviewed it.

In March 2000, ISACA's Academic Relations Committee established a task force of 15 individuals, predominantly full-time academics and IS professionals from 11 countries and five continents, charged with updating the original model curriculum. The task force realized that a course-based model curriculum was not suitable to serve the variety of educational institutions and thus developed an initial list of topics covering more than 350 issues. The topics were then pared down, based on urgency and relevance. The task force decided that a framework was needed to organize the topics and agreed that the CISA examination content domains could help accomplish this goal without necessitating the creation of a CISA preparation curriculum. Thus, the seven CISA content domains and their subtopics were used to provide a structure to organize the issues in the model curriculum.

The renewed *ISACA Model Curriculum for IS Audit and Control* was issued in 2004 and has since been used by institutions around the world to provide comprehensive programs targeted to meet the needs of the IS audit and assurance profession.

In 2008, the ISACA Academic Relations Committee revisited the 2004 model curriculum to:

- Determine whether it continued to meet the current needs of the IS audit profession
- Identify additional course components to fulfill those needs as well as course components that should be deleted
- Make any necessary revisions to align the *ISACA Model Curriculum for IS Audit and Control* to the most recent edition of COBIT and the current CISA content domains
- Encourage additional universities to have their programs reviewed by ISACA for the model curriculum alignment and, when that alignment is acknowledged, to post that information to the ISACA web site

As a result of this effort, *ISACA Model Curriculum for IS Audit and Control, 2nd Edition* was published.

In 2011, the Academic Program Subcommittee revisited the second edition because there were revisions made to the CISA Review Manual. These revisions were mainly due to changes to the CISA job practices, which required consolidation from six domains to five domains; this in turn required further changes to the subtopics. A work group was created to update the model curriculum and produce a third edition.

Creation of the Revised Model

While COBIT is a robust framework and was considered in the creation of the model, the CISA domains and knowledge statements continue to be a better fit for this academic exercise. It should be noted that the COBIT processes are integrated into the CISA content. (See Appendix 1. Relevance to the COBIT Conceptual Framework and CISA Content Domains.)

Guidance regarding the amount of educational coverage that should be devoted to each topic within the model curriculum needed to be clear enough that users of the model could benefit from it, 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 recommended hours of contact time for each topic, which is adaptable to the many different educational environments used globally. To develop these contact hour estimates, the Academic Program Subcommittee decided to provide guidance only at the domain level and not to suggest contact times for every 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 entry-level IS audit and control professionals would often include in excess of 300 contact hours. The 300 hours can be delivered in a variety of formats, including a series of eight-hour education seminars.

It was understood by the subcommittee that institutions would likely have areas in their curricula that might differ from areas included by other institutions. These differences are normal, and the ISACA model curriculum allows time for teaching these differing topics by identifying topical coverage requiring approximately 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 2. Suggested Supplemental Skills for IS Auditors) or focused on additional coverage of model topics.

An educational institution or professional organization can also structure its delivery system components (e.g., courses, modules) to include topics from anywhere within the model, not limited to any predetermined component structures. To determine alignment with the model, an institution or organization should create a mapping of where the model curriculum topics are delivered within its educational delivery system components. This mapping could be as simple as providing detailed syllabi of courses taught at a university and noting where items from the model curriculum are covered. (An alignment grid can be found in Appendix 3. Alignment Grid.)

Although it is important for the identified topics in the model curriculum to be covered, ISACA recognizes that educational entities, whether they are universities or professional organizations, 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. 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 since 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.

The model curriculum is designed to prepare an individual to pursue a degree with a focus on IS audit within the scope of a typical program. A typical undergraduate or graduate degree includes programs in information systems, accounting, commerce and finance. The topics in the model curriculum are designed to provide professional entry-level skills and capabilities (see Appendix 2. Suggested Supplemental Skills for IS Auditors).

3. Use

Alignment with the ISACA model curriculum entitles the program to be posted on the ISACA web site, and graduates of an aligned program qualify for one year of work experience toward the CISA certification.

The customary methods for delivering education differ greatly throughout the world. The original model, which was introduced in March 1998, has worked reasonably well in educational systems structured with a course focus. However, 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, which are recognized and valued in the professional workplace of those countries. In other countries, the education that would be similar to that promoted by the 1998 model is not offered by universities at all, but rather by professional society chapters, such as Chartered Accountants and ISACA chapters.

The *ISACA Model Curriculum for IS Audit and Control, 3rd Edition* covers topics proposed by a wide range of ISACA members with expertise in IS governance, assurance, security and control. 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 an entry-level position in the IS audit and control 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 Academic Program Subcommittee, the Model Curriculum work group and academic advocate reviewers. 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 a 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 level, not for every 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 an area, and perhaps little or no time to other subtopics. The educational institution can also structure its delivery system components (e.g., courses, modules) to include topics from anywhere within the model, not limited to any predetermined component structures.

As discussed previously, the topics and subtopics are organized according to the major domains for the CISA examination. Detailed descriptions of the topics and subtopics are included in the indicated figures that appear in chapter 4, *ISACA Model Curriculum for IS Audit and Control, 3rd Edition*.

The **Process of Auditing Information Systems** domain is divided into four topics. The fourth topic area has combined two of the CISA review manual topic areas: “Audit Reporting and Communications” with “Follow-up Reporting.” This covers the entire audit process from basic auditing concepts through reporting and follow-up stages of the audit. The objective of this domain is to ensure that the student has the knowledge necessary to provide audit services in accordance with IT audit standards and guidelines to assist an enterprise with protecting and controlling the information systems. Detailed descriptions of the topics and subtopics are listed in **figure 1**.

The **Governance and Management of IT** domain is divided into ten topic areas with subtopics for each that focus on the management of process IT areas such as human resources (HR), IT organizational structure legal issues, and standards and monitoring of assurance practices. Two topic areas have been combined: "Quality Management" with "IT Management of Controls." The main objective of this domain is for the student to understand that the necessary leadership and organizational structures and processes are in place to achieve the objectives and to support the enterprise's strategy. Detailed descriptions of the topics and subtopics are listed in **figure 2**.

The **Information Systems Acquisition, Development and Implementation** domain is divided into six topic areas that focus on business case development, project management and controls. The objective of this domains to ensure that students understand and can provide assurance that the practices of acquiring, developing, testing and implementing information systems meet the enterprise's strategies and objectives. Detailed descriptions and subtopics are listed in **figure 3**.

The **Information Systems Operations**, **Maintenance and Support** domain is divided into ten topic areas that focus on service level management, maintenance of information systems, problem and incident management, change and configuration management, and backup and restoration of systems. The objective of this domain is to ensure that students understand and can provide assurance that the practices for systems operations and maintenance meet the enterprise's strategies and objectives. Detailed descriptions and subtopics are listed in **figure 4**.

The **Protection of Information Assets** domain is divided into five topic areas that focus on design and implementation of system and security controls, data classification, physical access, and the process of retrieving and disposing of information assets. The objective of this domain is to ensure that students understand and can provide assurance that the enterprise's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets. Detailed descriptions and subtopics are listed in **figure 5**.

To determine alignment with the model, the educational institution should create a map of where the model curriculum topics are delivered within its educational delivery system components. The mapping process steps are detailed in **figure 8** in Appendix 3. Alignment Grid, which provides a form to map an academic program to the model.

4. ISACA Model Curriculum for IS Audit and Control, 3^{rd} Edition

The topics covered by the model are grouped into five content domains. These domains are divided 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, which **total 250 hours**. Each domain, its topics, subtopics and the required hours for each topic are listed in **figures 1** through **5**.

Domain 1: The Process of Auditing Information Systems

Knowledge Objective

Developing the knowledge necessary to provide audit services in accordance with IT audit standards to assist the enterprise with protecting and controlling information systems.

Learning Objectives

- Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the enterprise.
- Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
- Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
- Conduct follow-ups or prepare status reports to ensure appropriate actions have been taken by management in a timely manner.

Figure 1—The Process of Auditing Information Systems Domain

Topic	Hours	Subtopic
Risk-based IT audit strategy	**7**	Risk assessment concepts
		Control objectives and information system controls
		Applicable laws and regulations affecting the audit scope
		Quality assurance systems and frameworks
		Technology and audit environment changes
Specific audit planning	**8**	Audit charter/engagement letters
		ISACA—IT audit and assurance standards, guidelines, assurance guide, tools and techniques, code of professional ethics
		Audit planning techniques and project management
		Audit planning steps
		Business processes (e.g., accounting, HR)
		Performing risk assessments
IT audit standards	**18**	Evidence collection techniques (e.g., observation, inquiry, interviews, inspection, data analysis)
		Sampling methodologies
		Internal controls and control types (preventive, detective, etc.)
		Steps to determine regulatory requirements
		Procedures for testing and evaluating internal controls
		Fraud detection techniques and tools
		Use of self assessments
Audit reporting, communications and follow-up	**7**	Reporting and communication techniques
		Exit interviewing
		Presentation and reporting techniques
Total	**40**	

Domain 2: Governance and Management of IT

Knowledge Objective

Understands and can provide assurance that the enterprise has the structure, policies, accountability mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT.

Learning Objectives

- Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the enterprise's strategies and objectives.
- Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the enterprise's strategies and objectives.
- Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the enterprise's strategies and objectives.
- Evaluate the enterprise's IT policies, standards and procedures, and the processes for their development, approval, implementation, maintenance and monitoring to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- Evaluate the adequacy of the quality management system (QMS) to determine whether it supports the enterprise's strategies and objectives in a cost-effective manner.
- Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance) for compliance with the enterprise's policies, standards and procedures.
- Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the enterprise's strategies and objectives.
- Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the enterprise's strategies and objectives.
- Evaluate risk management practices to determine whether the enterprise's IT-related risk is properly managed.
- Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
- Evaluate the enterprise's business continuity plan (BCP) to determine the enterprise's ability to continue essential business operations during the period of an IT disruption.

Figure 2—Governance and Management of IT Domain

Topic	Hours	Subtopic
IT governance structures	**6**	IT strategy, policies, standards and procedures for an enterprise and the essential elements of each
		IT governance, security and control frameworks, related standards, guidelines and practices
		IT audit role in governance
IT organizational structure and HR	**6**	Committee structures with their roles and responsibilities
		Organizational structure, roles and responsibilities related to IT
		HR policies such as hiring, performance and training
		Segregation of duties and mapping to roles and responsibilities
IT strategy and direction	**6**	Organizational technology direction
		Organizational business strategic direction and how IT aligns with it
IT policies, standards and procedures	**6**	Processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures for an enterprise and the essential elements of each
		Regulatory and legal requirements impacting the enterprise
QMS and IT management of controls	**5**	Quality management systems
		Investment and financial allocation techniques
Monitoring and assurance practices	**6**	Maturity modeling and process capability assessment techniques
		Performance measurement techniques (e.g., balance score card techniques)
IT resource management	**6**	Process optimization techniques
		Sourcing practices
		Global sourcing practices
		Service and operating level agreements (OLAs)
IT contracting strategies and policies	**6**	Third-party and outsourcing practices and techniques
		Change management techniques
		Supplier/vendor selection, contract and relationship management
Risk management practices	**6**	Business impact analysis (BIA) and risk management practices
		Enterprise risk management (ERM) system
Business continuity planning (BCP)	**7**	Standards and procedures for the development and maintenance of the BCP and the testing methods
Total	**60**	

Domain 3: Information Systems Acquisition, Development and Implementation

Knowledge Objective

Understands and can provide assurance that the practices for the acquisition, development, testing and implementation of information systems meet the enterprise's strategies and objectives.

Learning Objectives

- Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
- Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risk to the enterprise.
- Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
- Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the enterprise's policies, standards, procedures and applicable external requirements.
- Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the enterprise's requirements are met.
- Conduct postimplementation reviews of systems to determine whether project deliverables, controls and the enterprise's requirements are met.

Figure 3—Information Systems Acquisition, Development and Implementation Domain

Topic	Hours	Subtopic
Business case development	**6**	Benefits realization techniques (total cost of ownership [TCO], return on investment [ROI])
		Project and portfolio management techniques
Project management practices	**8**	Project governance mechanisms
		Project control frameworks, practices and tools
		Project risk management practices
Project reviews	**6**	Project success factors and risk
		Risk management practices applied to projects
Develop project controls	**18**	IT architecture related to data, applications and technology (e.g., distributed applications, web-based applications, web services, n-tier applications)
		Acquisition practices
		Requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis vulnerability management, security requirements)
		Control objectives and techniques that ensure completeness, validity, accuracy and authorization of transactions and data (e.g., COBIT)
		Systems development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)
		Testing methodologies and practices related to information systems
Information systems implementation and migration	**7**	Configuration and release management related to systems development
		Systems migration and infrastructure deployment practices and data conversion tools, techniques and procedures
Postimplementation reviews	**5**	Postimplementation review objectives and practices (e.g., project closure, control implementation, benefits realization and performance measurement)
Total	**50**	

Domain 4: Information Systems Operations, Maintenance and Support

Knowledge Objective

Understands and can provide assurance that the IT service management practices will ensure the delivery of the level of services required to meet the enterprise's objectives.

Learning Objectives

- Conduct periodic reviews of information systems to determine whether they continue to meet the enterprise's objectives.
- Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
- Evaluate third-party management practices to determine whether the levels of controls expected by the enterprise are being adhered to by the provider.
- Evaluate operations and end-user procedures to determine whether scheduled and nonscheduled processes are managed to completion.
- Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the enterprise's objectives.
- Evaluate data administration practices to determine the integrity and optimization of databases.
- Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the enterprise's objectives.
- Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.
- Evaluate change, configuration and release management practices to determine whether scheduled and nonscheduled changes made to the enterprise's production environment are adequately controlled and documented.

Figure 4—Information Systems Operations, Maintenance and Support Domain

Topic	Hours	Subtopic
Information systems reviews	**5**	Technology concepts related to hardware and network components, system software and database management systems
		Systems resiliency tools
Service level management practices	**7**	Service level management practices and components within a service level agreement (SLA)
Third-party management practices	**7**	Software licensing and inventory practices
		Monitoring techniques for third-party compliance with enterprise internal controls (SSAE16 and SOC reporting, IAE 3402)
End-user procedures and operations	**5**	Operations and end-user procedures for managing scheduled and nonscheduled processes
Maintenance of information systems	**3**	Control techniques that ensure the integrity of system interfaces
Data administration practices	**3**	Database administration practices
Capacity and performance monitoring	**5**	Capacity planning and related monitoring tools and techniques
		Systems performance monitoring processes and tools (e.g., network analyzers, system utilization reports, load balancing)
Problem and incident management	**6**	Problem and incident management practices (e.g., help desk, escalation procedures, tracking and monitoring)
Change, configuration and release management	**4**	Processes for managing scheduled and nonscheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices
Backup and restoration of systems	**5**	Data backup, storage, maintenance, retention and restoration practices
Total	**50**	

Domain 5: Protection of Information Assets

Knowledge Objective

Understands and can provide assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets.

Learning Objectives

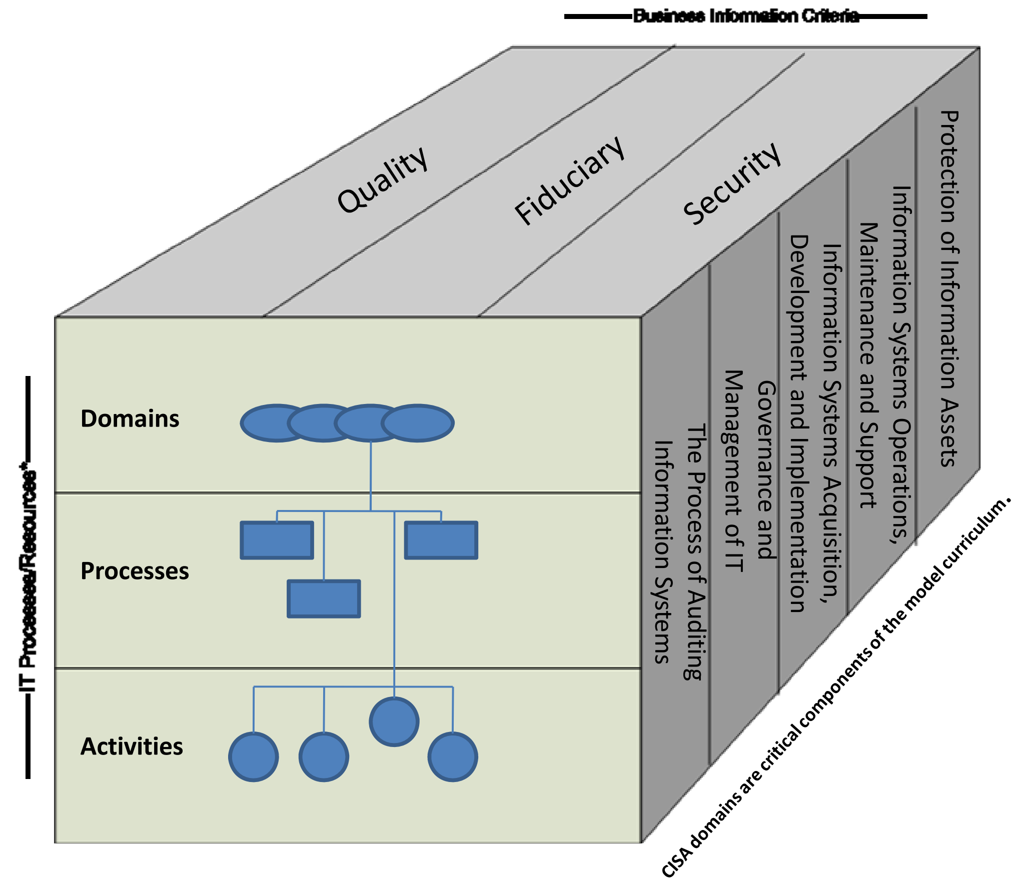
- Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
- Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
- Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization’s policies, standards, procedures and applicable external requirements.
- Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
- Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data and softcopy media) to determine whether information assets are adequately safeguarded.

Figure 5—Protection of Information Assets Domain

Topic	**Hours**	**Subtopic**
Information security policies, standards and procedures and generally accepted practices	**7**	Approaches and techniques for the design, implementation and monitoring of security controls, including awareness programs
		Incident management techniques
		Risk and control associated with data leakage
		Evidence preservation techniques for forensics investigations
Design, implementation and monitoring of system and logical security controls to verify confidentiality, integrity, availability (CIA)	**15**	Logical access controls for the identification, authentication and restriction of users to authorize functions and data
		Risk and controls associated with virtual systems
		Network and Internet security devices, protocols, techniques
		Detection tools and control techniques
		Security testing techniques(intrusion testing, vulnerability scanning)
		Encryption tools and techniques
		Public key infrastructure
		Risk associated with peer-to-peer computing
		Controls and risk associated with the use of mobile and wireless devices
Data classification processes and procedures	**7**	Data classification standards and supporting procedures
		Procedures for storing, retrieving, transporting and disposal of confidential information assets
Physical access and environmental controls	**7**	Physical access controls for the identification, authentication and restriction of users to authorized facilities
		Environmental protection devices and supporting practices
Processes for storing, retrieving, transporting and disposing of information assets	**14**	Procedures for storing, retrieving, transporting and disposal of confidential information assets
		Encryption-related techniques
Total	**50**	
Grand Total	**250**	Figures 1 through 5

Appendix 1. Relevance to the COBIT Conceptual Framework and CISA Content Domains

Figure 7—Relevance of the *ISACA Model Curriculum for IS Audit and Control* to the COBIT Conceptual Framework and CISA Content Domains


Business Information Criteria
Quality
Fiduciary
Security
Protection of Information Assets
Information Systems Operations, Maintenance and Support
Information Systems Acquisition, Development and Implementation
Governance and Management of IT
The Process of Auditing Information Systems
IT Processes/Resources*
Domains
Processes
Activities
CISA domains are critical components of the model curriculum.

*IT resources involve applications, information, infrastructure and people.

The topics in the *ISACA Model Curriculum for IS Audit and Control, 3rd Edition*, are designed to provide professional entry-level skills and capabilities in business/commerce areas. The five ISACA content domains and their subtopics were used to provide a structure to organize the issues in the model. IT processes are addressed by COBIT, which is integrated into the CISA content domains (**figure 7**).

Appendix 2. Suggested Supplemental Skills for IS Auditors

The following competencies are not considered directly in the IS audit profile because they are not specific to IS audit, but they are required in most professions.

Analytical skills—The ability to visualize, articulate and solve complex problems and concepts, and make decisions that make sense based on available information. Such skills include demonstration of the ability to apply logical thinking to gathering and analyzing information, designing and testing solutions to problems, and formulating plans.

Client maintenance—Includes the ability to effectively maintain a client during a permitted length of time for audit services and also cultivate the sustenance for the business of the professional

Managerial communications and/or public speaking—Includes the communication skills that are employed when discussing audit scope, findings and recommendations

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

Negotiation skills and/or personal selling—Includes the ability to convince management to implement recommendations for positive change

Business writing—Includes the ability to produce concise, understandable and usable reports, presentation materials, and other written communications

Industrial psychology and/or behavioral science—Includes the ability to understand and effectively manage human behavior throughout the audit process

Project management/time budgeting—Includes the ability to effectively and efficiently manage time and tasks during audits. Auditors are frequently evaluated on covering specific scopes within time lines and budgets.

Team building and team leading—Includes the ability to effectively manage team activities with proper coordination and utilization of knowledge and skills of individual team members in the performance of an IS audit

Appendix 3. Alignment Grid

To map a program to the *ISACA Model Curriculum for IS Audit and Control, 3rd 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 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.
- Make sure the current textbook supporting the classes and the visual media/projects that may be 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 what is taught in 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 8**.

Figure 8—Mapping Process Steps

1	Identify all direct and support courses that apply to the program.
2	Ensure that the current syllabi or expanded course outlines and support materials for the courses are accessible. It takes approximately 20 hours to complete the mapping, if expanded course outlines are available from which information can be extracted. (Note: The topics are all interlinked—Domain 2 drives much of Domain 4—they are very much related.)
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 that 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 50 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.

Submit the following completed tables to ISACA for review by e-mail at *research@isaca.org*, fax at +1.847.253.1443, or mail at: Technical Research Manager for the Academic Program Sub-committee, 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 IS Audit and Control*, 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 CISA certification.

Domain 1—The Process of Auditing Information Systems Alignment Grid				
Topic	**Hours**	**Subtopic**	**Course(s) covering the Subtopic**	**Hours**
Risk-based IT audit strategy	**7**	Risk assessment concepts		
		Control objectives and information system controls		
		Applicable laws and regulations affecting the audit scope		
		Quality assurance systems and frameworks		
		Technology and audit environment changes		
Specific audit planning	**8**	Audit charter/engagement letters		
		ISACA—IT audit and assurance standards, guidelines, assurance guide, tools and techniques, code of professional ethics		
		Audit planning techniques and project management		
		Audit planning steps		
		Business processes (e.g., accounting, HR)		
		Performing risk assessments		
IT audit standards	**18**	Evidence collection techniques (e.g., observation, inquiry, interviews, inspection, data analysis)		
		Sampling methodologies		
		Internal controls and control types (preventive, detective, etc.)		
		Steps to determine regulatory requirements		
		Procedures for testing and evaluating internal controls		
		Fraud detection techniques and tools		
		Use of self assessments		
Audit reporting and communications and follow-up	**7**	Reporting and communication techniques		
		Exit interviewing		
		Presentation and reporting techniques		
Total	**40**			

Domain 2—Governance and Management of IT Alignment Grid				
Topic	**Hours**	**Subtopic**	**Course(s) Covering the Subtopic**	**Hours**
IT governance structures	**6**	IT strategy, policies, standards and procedures for an enterprise and the essential elements of each		
		IT governance, security and control frameworks, related standards, guidelines and practices		
		IT audit role in governance		
IT organizational structure and HR	**6**	Committee structures with their roles and responsibilities		
		Organizational structure, roles and responsibilities related to IT		
		HR policies such as hiring, performance and training		
		Segregation of duties and mapping to roles and responsibilities		
IT strategy and direction	**6**	Organizational technology direction		
		Organizational business strategic direction and how IT aligns with it		
IT policies, standards and procedures	**6**	Processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures for an enterprise and the essential elements of each		
		Regulatory and legal requirements impacting the enterprise		
QMS and IT management of controls	**5**	Quality management systems		
		Investment and financial allocation techniques		
Monitoring and assurance practices	**6**	Maturity modeling and process capability assessment techniques		
		Performance measurement techniques (e.g., balance score card techniques)		
IT resource management	**6**	Process optimization techniques		
		Sourcing practices		
		Global sourcing practices		
		Service and OLAs		
IT contracting strategies and policies	**6**	Third-party and outsourcing practices and techniques		
		Change management techniques		
		Supplier/vendor selection, contract and relationship management		
Risk management practices	**6**	Business impact analysis (BIA) and risk management practices		
		Enterprise risk management (ERM) system		
Business continuity planning (BCP)	**7**	Standards and procedures for the development and maintenance of the BCP and the testing methods		
Total	**60**			

Domain 3—Information Systems Acquisition, Development and Implementation Alignment Grid				
Topic	**Hours**	**Subtopic**	**Course(s) Covering the Subtopic**	**Hours**
Business case development	**6**	Benefits realization techniques (total cost of ownership [TCO], return on investment [ROI])		
		Project and portfolio management techniques		
Project management practices	**8**	Project governance mechanisms		
		Project control frameworks, practices and tools		
		Project risk management practices		
Project reviews	**6**	Project success factors and risk		
		Risk management practices applied to projects		
Develop project controls	**18**	IT architecture related to data, applications and technology(e.g., distributed applications, web-based applications, web services, *n-tier* applications)		
		Acquisition practices		
		Requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis vulnerability management, security requirements)		
		Control objectives and techniques that ensure completeness, validity, accuracy and authorization of transactions and data (e.g., COBIT)		
		Systems development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)		
		Testing methodologies and practices related to information systems		
Information systems implementation and migration	**7**	Configuration and release management related to systems development		
		Systems migration and infrastructure deployment practices and data conversion tools, techniques and procedures.		
Postimplementation reviews	**5**	Postimplementation review objectives and practices (e.g., project closure, control implementation, benefits realization and performance measurement)		
Total	**50**			

Domain 4—Information Systems Operations, Maintenance and Support Alignment Grid				
Topic	**Hours**	**Subtopic**	**Course(s) Covering the Subtopic**	**Hours**
Information systems reviews	**5**	Technology concepts related to hardware and network components, system software and database management systems		
		Systems resiliency tools		
Service level management practices	**7**	Service level management practices and components within a service level agreement (SLA)		
Third-party management practices	**7**	Software licensing and inventory practices		
		Monitoring techniques for third-party compliance with enterprise internal controls (SSAE16 and SOC reporting, IAE3402)		
End-user procedures and operations	**5**	Operations and end-user procedures for managing scheduled and nonscheduled processes		
Maintenance of information systems	**3**	Control techniques that ensure the integrity of system interfaces		
Data administration practices	**3**	Database administration practices		
Capacity and performance monitoring	**5**	Capacity planning and related monitoring tools and techniques		
		Systems performance monitoring processes and tools (e.g., network analyzers, system utilization reports, load balancing)		
Problem and incident management	**6**	Problem and incident management practices (e.g., help desk, escalation procedures, tracking and monitoring)		
Change, configuration and release management	**4**	Processes for managing scheduled and nonscheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices		
Backup and restoration of systems	**5**	Data backup, storage, maintenance, retention and restoration practices		
Total	**50**			

Domain 5—Protection of Information Assets Alignment Grid

Topic	Hours	Subtopic	Course(s) Covering the Subtopic	Hours
Information security policies, standards and procedures and generally accepted practices	**7**	Approaches and techniques for the design, implementation and monitoring of security controls, including awareness programs		
		Incident management techniques		
		Risk and control associated with data leakage		
		Evidence preservation techniques for forensics investigations		
Design, implementation and monitoring of system and logical security controls to verify confidentiality, integrity, availability (CIA)	**15**	Logical access controls for the identification, authentication and restriction of users to authorize functions and data		
		Risk and controls associated with virtual systems		
		Network and Internet security devices, protocols, techniques		
		Detection tools and control techniques		
		Security testing techniques(intrusion testing, vulnerability scanning)		
		Encryption tools and techniques		
		Public key infrastructure		
		Risk associated with peer-to-peer computing		
		Controls and risk associated with the use of mobile and wireless devices		
Data classification processes and procedures	**7**	Data classification standards and supporting procedures		
		Procedures for storing, retrieving, transporting and disposal of confidential information assets		
Physical access and environmental controls	**7**	Physical access controls for the identification, authentication and restriction of users to authorized facilities		
		Environmental protection devices and supporting practices		
Processes for storing, retrieving, transporting and disposing of information assets	**14**	Procedures for storing, retrieving, transporting and disposal of confidential information assets		
		Encryption-related techniques		
Total	**50**			
Grand Total	**250**	Domains 1 through 5		

Appendix 4. References

Gallegos, Fred; Alan Lord; "ISACA Model Curriculum 2004: Continuing to Invest in our Future," *Information Systems Control Journal*, Volume 6, 2004

ISACA, CISA Examination Areas, USA, 2011, *www.isaca.org/cisa*

ISACA, *ISACA Model Curriculum for IS Audit and Control, 2nd Edition*, USA, 2008

ISACA, *ISACA Model Curriculum for Information Security Management*, USA, 2008

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

Lord, A. T.; "ISACA Model Curriculum 2004," *International Journal of Accounting Information Systems*, Volume 5, 2 July 2004