Information Systems Audit and Control Association®

ISACA Model Curriculum for IS Audit and Control

Information Systems Audit and Control Association®
With more than 35,000 members in more than 100 countries, the Information Systems Audit and Control Association (ISACA®) (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*™, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation earned by more than 35,000 professionals since inception, and Certified Information Security Manager™ (CISM™) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

Disclaimer
The Information Systems Audit and Control Association and the authors have designed and created this publication, entitled *ISACA Model Curriculum for IS Audit and Control* primarily as an educational resource for academics, assurance, and control professionals. ISACA and the authors make no claim that use of this publication will assure a successful outcome. This publication should not be considered inclusive of any 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 procedure or test, security and control professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology environment.

Copies of the model curriculum are freely available to all ISACA members, colleges and universities and may be downloaded from *www.isaca.org*. Printed copies are available for a small fee through the ISACA Bookstore. E-mail *bookstore@isaca.org* for details.

Disclosure

Information System Audit and Control Association
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*

ISBN 1-893209-85-7
ISACA Model Curriculum for IS Audit and Control
Printed in the United States of America

Acknowledgments

ISACA wishes to recognize:

The Board of Directors for its support

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young, LLP, USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Ricardo J. Bria, CISA, SAFE Consulting, Spain, Vice President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Vice President
Howard Nicholson, CISA, Mortgage Choice, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank Yam, CISA, CIA, CCP, CFE, Focus Strategic Group Inc., Hong Kong, Vice President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Paul A. Williams, FCA, MBCS, Paul Williams Consulting, UK, Past International President
Emil G. D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, USA, ITGI Trustee
Ronald Saull, CSP, The Great-West Life Assurance Company, Canada, ITGI Trustee

Model Curriculum Task Force Members

Chair, Alan T. Lord, Ph.D., CISA, CPA, Bowling Green State University, USA
José Roberto Alpízar Fallas, CPA, Universidad de Costa Rica, Costa Rica
Peter Best, Ph.D., CPA, CA, FCP, Q.U.T. Accountancy, Australia
J. Efrim Boritz, Ph.D., CISA, CA, FCA, University of Waterloo, Canada
Allen Bragan, CISA, CPA, CGFM, DABFA, University of Alabama, USA
Richard Fisher, CISA, CA, CMA, Lincoln University, New Zealand
Frederick Gallegos, CISA, CDE, CGFM, California State Polytechnic University at Pomona, USA
S. Michael Groomer, Ph.D., CISA, CCP, CPA, CITP, Indiana University, USA
Rodger Jamieson, Ph.D., CA, CPA, University of New South Wales, Australia
Dong Soo Lee, CISA, Jeongwoo Infotech Co. Ltd., Korea
Edmundo Marroquin Tovar, CISA, Universidad Panamericana, Mexico
K. Subramanian, Ph.D., CAG/NIC, India
Wim Van Grembergen, Ph.D., University of Antwerp, Belgium
Margaret E. van Biene-Hershey, Vrije University, The Netherlands
G. (John) van der Pijl, Ph.D., Erasmus University, The Netherlands
Hiroshi Yoshida, Ph.D., Nagoya Bunri University, Japan

Academic Relations Committee

Chair, Alan T. Lord, Ph.D., CISA, CPA, Bowling Green State University, USA
Anjay Agarwal, CISA, ACS, CA, CFE, CIA, Anjay Agarwal & Co., India
Rosemary Amato, CISA, CMA, CPA, Deloitte & Touche LLP, The Netherlands
Ashutosh Deshmukh, Ph.D., CISA, CA, CFE, Pennsylvania State University, USA
Peter Edwards, Ph.D., University of Sydney, Australia
Regina Garza Roche, Gobierno del Estado de Yucatán Secretaria De la Contraloria General, México
Wanbil William Lee, Caritas Francis Hsu College, Hong Kong
Balint Molnar, Ph.D., CISA, MTA IT Foundation, Hungary
Randall Craig Reid, Ph.D., CISA, CISSP, University of West Florida, USA
Kaustav Sen, Ph.D., CISA, Pace University, USA
Smita Dilip Totade, Ph.D., CISA, CISM, FIEI, SMCSI, National Insurance Academy, India
Woon (Dan) Kwan Tse, CISA, CISM, CISSP, City University of Hong Kong, Hong Kong
Markus Warncke, CISA, CIA, CFE, CCSA, Villeroy & Boch AG, Germany

Table of Contents

1. Background

ISACA History

The evolution of information technology (IT) affects the business environment in many significant ways. 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 by the 1969 founding of what is now known as the Information Systems Audit and Control Association (ISACA).

ISACA was formed, and continues to exist today, to meet the unique and diverse high 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 35,000 consultants, academics, security professionals, IS auditors and senior executives who make up ISACA have established 160 chapters spread among 100 countries. ISACA's IS Auditing and IS Control Standards are followed by practitioners worldwide and its Certified Information Systems Auditor® (CISA®) certification is recognized globally and has been earned by more than 35,000 professionals. The newer Certified Information Security Manager® (CISM®) certification uniquely targets the information security management audience. In addition, ISACA publishes the *Information Systems Control Journal®*, a leading technical journal in the information control field, and sponsors a series of international conferences focusing on technical and managerial topics. Together, ISACA and its affiliate, the IT Governance Institute (ITGI), lead the IT control community and serve its practitioners by providing the elements needed by IT professionals in an ever-changing worldwide environment.

Need for the Model Curriculum

For a number of years, many employers have been seeking to fill positions with accounting and assurance professionals who possess a substantial background in audit, control and IT, and this demand is expect to grow in the future. Often employers have had difficulty in locating a sufficient number of adequately prepared candidates for the open positions. The professionals who do have the requisite background have usually obtained their formal IS auditing 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 organization, and it is most appropriate where the technology presented has been adopted and implemented by a particular organization. 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 organizations or vendors.* This method is available to professionals from many different organizations and it is valuable in presenting information that is new, or for exploring various approaches to IS auditing

problems. In the workshop/seminar environment, a peer group can share perspectives not available from a single instructor. However, workshops/seminars are usually more expensive, take time away from the office, and are typically available only to professionals who are already employed in the workforce. Also, most seminars are limited in topical coverage and do not provide the in-depth, technical, hands-on competence required in IS auditing. ISACA is well known for developing and offering high-quality workshops and seminars.

- *Participation in university degree 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 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 upon 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, IS or computer science) and then perhaps one or two courses in a second area, such as IS or accounting, usually without coordination of course content among the various disciplines.

IS auditors need to be able to cope with the pace of rapid technological changes and update themselves regularly with competent technical knowledge. Recent events, government regulations and changes in business processes have affected the role of IS audit and the methodologies 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 communicate clearly 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 auditing 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 upon 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 universities can educate students for careers in the IS audit and control profession 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 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 organization, 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 (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 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 compliance mapping to the model. Format, arrangement and content of the proposed curriculum will vary depending on university accreditation and government requirements.

Conclusion

The IS audit and control profession continues to evolve. ITGI's *Control Objectives for Information and related Technology* (COBIT®) 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 required skills and knowledge that the profession needs. The ISACA model curriculum provides universities with a basic framework of the education required to develop the skills needed to be employable in the profession.

In the information-based business environment, business 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 2004 Model Curriculum for Information Systems Audit and Control* can be viewed as a reasonably comprehensive set of topics for an ideal program for IS audit and control. The model curriculum 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 interested educational institutions worldwide that are developing a curriculum in IS audit and control.

2. Development of the ISACA Model Curriculum

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 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. The model was based on the needs and the expectations of the IS audit profession and the prior research of academics, practitioners, audit organizations and professional societies. The model curriculum was considered a living document, to be regularly updated.

Over the last several years, issues were identified leading to the conclusion that the model curriculum needed updating. Technology advancement and the increased computer literacy of students made some of the recommended courses and the strict course approach outdated. New technologies important for IT assurance professionals to have in their educational background were not in existence when the model was created. There were also topics emphasized in the model that are now an accepted part of the computer literacy of most students. The model was presented in terms of courses that would be offered by institutions, but currently, universities and professional organizations deliver educational programs using a wide variety of formats and structures.

In March 2000, ISACA's Academic Relations Committee established a task force charged with updating the original model curriculum. A global recruiting effort was launched to identify qualified and interested members of ISACA to form this task force. Ultimately, 15 individuals accepted invitations to serve. The task force was predominately composed of full-time academics, although several professional IS auditors who were interested in the development of the model also served. During the task force selection process, an effort was made to reflect the global nature of the ISACA membership, resulting in a task force populated by members representing 11 countries and five continents.

The mission statement for the new Model Curriculum Task Force was to:

- Determine whether the current model curriculum continues to meet the current needs of the IS audit profession
- Identify additional course components to fulfill those needs and courses that should be deleted
- Update the specific course descriptions in the appendix of the current model
- Make any necessary revisions to reconcile the model curriculum to the most recent edition of COBIT and the current CISA content areas
- Formulate a plan to stimulate current and future interest at universities in the ISACA model curriculum
- Create a procedure for universities to have their programs reviewed by ISACA for model curriculum compliance and, when that compliance is acknowledged, to post that information to the ISACA web site
- Establish a renewal process for reevaluation of university programs for compliance with the ISACA model curriculum

Once the task force was initiated, it quickly concluded that a better alternative to the "course focus," which the original model utilized, would be to develop a model that presented topical areas to be covered in the program and allow each educational organization or environment to decide the manner in which the educational content would be delivered. This change meant that the task force would not merely be updating the 1998 model, but would instead be creating a new/revised model that could be adopted more readily on a global basis by traditional education institutions and professional organizations.

Creation of the Revised Model

An initial list of topics covering more than 350 issues was developed. The topics were then pared down, based on urgency and relevance. The task force decided that a framework was needed with which to organize the topics. The task force agreed that the CISA examination content areas could provide a framework to organize the topics without resulting in the creatiion of a CISA preparation curriculum. Thus, the seven CISA content areas and their subtopics were used to provide a structure to organize the issues in the model curriculum. The seven major content (domain) areas in the CISA examination are:

- Audit process
- Management planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management

While COBIT was considered in the creation of the model, and although it is a robust framework, the CISA content was found to be a better fit for this academic exercise. It should be noted that the COBIT processes are integrated into the CISA content areas. (See Appendix 1, Relevance of the ISACA Model Curriculum to the COBIT Conceptual Framework and CISA Content Areas.)

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 used 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 attempt 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 entry-level IS audit and control 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 task force 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 allows time for teaching these differing topics by identifying topical coverage requiring only 244 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 and not be limited to any predetermined component structures. To determine compliance 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. (A compliance grid can be found in Appendix 3, Compliance Grid for the ISACA Model Curriculum for IS Audit and Control.)

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. For universities with a business education program in the US, use of the Association to Advance Collegiate Schools of Business (AACSB) standards is an acceptable model for curriculum design since the accreditation process is 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 compliance 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 and graduate degree includes programs in IS, 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 of the ISACA Model Curriculum

Compliance with the ISACA model curriculum 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 Certified Information System Auditor (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.

ISACA 2004 Model Curriculum for Information Systems Audit and Control 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 toward 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 upon the experience and knowledge of the ISACA Academic Relations Committee, the Model Curriculum Task Force and participants from a COBIT in Academia workshop. (The workshop participants were academics from around the world with experience teaching COBIT in the classroom.) 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 an area 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 not be limited to any predetermined component structures.

As discussed previously in this document, 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.

The audit process domain is divided into eight topic areas, each with two to nine different subtopics. The topics cover the entire audit process from basic auditing concepts through the reporting and follow-up stages of the audit. Detailed descriptions of the topics and the subtopics are listed in **figure 1**.

The management planning and organization of IS domain is divided into five topic areas that have from three to nine subtopics each. This domain focuses on the management of IS process areas such as projects, infrastructure, human resources, legal issues and standards. Detailed descriptions of the topics and the subtopics are listed in **figure 2**.

The technical infrastructure and operational practices domain also includes subtopics categorized under a topic called service center management. It includes discussions about operating and systems software decisions, network communication alternatives, IT architecture options, and management of service centers. Detailed descriptions of the topics and subtopics are listed in **figure 3**.

The protection of information assets domain includes the logical security principles as well as many network security issues, such as firewalls, intrusion detection systems and encryption considerations. Detailed descriptions of these topics and the subtopics are listed in **figure 4**.

Figure 5 provides the topics and subtopics for the disaster recovery and business continuity domain. These include not only management's responsibilities, but also the assurance professional's role in these issues and the importance of insurance coverage as part of the plan.

The business application system development, acquisition, implementation and maintenance domain includes topics related to enterprise resource planning software, the many issues related to database management and administration, the systems development life cycle and software development considerations. Detailed descriptions of the topics and the subtopics are listed in **figure 6**.

The last domain, business process evaluation and risk management, has only one topic area—the audit and development of application controls. There are four subtopics relating to input, output, processing controls and application systems documentation. These are listed in **figure 7**.

To determine compliance 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 9** in Appendix 3, Compliance grid for the ISACA Model Curriculum for IS Audit and Control, which provides a form to map an academic program to the model. Sample mappings are provided in Appendix 4, Examples of Mapping Programs to the ISACA Model Curriculum Compliance Grid, using data from actual schools.

4. ISACA Model Curriculum for IS Audit and Control

The topics covered by the model are grouped into seven content 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. Each domain, its topics, subtopics and the required hours for each topic are listed in **figures 1** through **7**.

Figure 1—Audit Process Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
IS Audit Function Knowledge	6	Laws and regulations: audit charter
		Nature of audit: demand for audits (e.g., agency theory, insurance hypothesis, information hypothesis)
		Nature of IS audit: need for control and audit of computer-based IS
		Types of audit and auditor: IS, external, internal, government/public sector
		IS auditor responsibility, authority and accountability: audit charter, outsourcing of IS audit activities
		Regulation and control of IS audit: ISACA standards, guidelines, Code of Professional Ethics; laws; regulations
Fundamental Auditing Concepts	7	Materiality: application of materiality for IS audit compared to materiality for financial statement audit
		Evidence: types of evidence; meaning of sufficient, reliable, relevant evidence
		Independence: need for independence in attitude and appearance, situations that may impair independence
		Audit risk: inherent risk, control risk, detection risk
		IS and general audit responsibilities for fraud
		Assurance
Standards and Guidelines for IS Auditing	5	Knowledge of ISACA Code of Professional Ethics
		Review of current ISACA IS Auditing Standards and Guidelines
		Standards and guidelines specific to a region/country: ACM, AGA, AICPA, AITP, IFAC, IIA, ISO, NIA (See appendix 5, Acronyms for full names.)
		IS audit practices and techniques
Internal Controls Concepts Knowledge	13	Relevance, structure and indicators of effective IT governance for organizations and IS auditors; IT governance structure
		Internal control objectives; internal control and documentation of IS, COCO, COSO, King, Sarbanes-Oxley Act of 2002, SAS94
		Control classifications: preventive, detective, compensating/corrective
		General controls: organizational, security, general operating and disaster recovery, development, documentation
		Application controls: control objectives; classifications of application controls, e.g., computerized/manual, input/processing/output, preventive/detective/corrective, audit trails
		COBIT: Relevance for organizations and IS auditors; structure of COBIT
Audit Planning Process	7	Strategic/tactical audit planning
		Engagement letter: purpose and content of engagement letters
		Risk assessment: risk-based auditing; risk assessment methods; standards such as AS-NZ 4360, CRAMM
		Preliminary evaluation of internal controls: information gathering and control evaluation techniques
		Audit plan, program and scope: compliance vs. substantive testing, application of risk assessment to audit plan
		Classification, scope of audits: e.g., financial, operational, general, application, OS, physical, logical

Figure 1—Audit Process Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
Audit Management	5	Resource allocation/prioritization/planning/execution/reassignments
		Evaluating audit quality/peer reviews
		Best practice identification
		Computer information systems (CIS) audit career development
		Career path planning
		Performance assessment
		Performance counseling and feedback
		Training (internal/external)
		Professional development (certifications, professional involvement, etc.)
Audit Evidence Process	12	Evidence: sufficient, reliable, relevant, useful
		Evidence gathering techniques, e.g., observation, inquiry, interview, testing
		Compliance vs. substantive testing: nature of and difference between compliance and substantive testing, types of compliance test, types of substantive test
		Sampling: sampling concepts, statistical and nonstatistical approaches, design and selection of samples, evaluation of sample results
		Computer-assisted audit techniques (CAATs): need for, types of, planning for and using CAATs; continuous online auditing approach
		Documentation: relationship with audit evidence; uses of documentation; minimum content; custody, retention, retrieval
		Analysis: judge the materiality of findings, identify reportable conditions, reach conclusions
		Review: provide reasonable assurance that objectives have been achieved
Audit Reporting Follow-up	3	Form and content of audit report: purpose, structure and content, style, intended recipient, type of opinion, consideration of subsequent events
		Management actions to implement recommendations
Total Hours	**58**	

Figure 2—Management, Planning and Organization of IS Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
IS/IT Management	10	IT project management
		Risk management: economic, social, cultural, technology risk management
		Software quality control management
		Management of IT infrastructure, alternative IT architectures, configuration
		Management of IT delivery (operations) and support (maintenance)
		Performance measurement and reporting: IT balanced scorecard
		Outsourcing
		Quality assurance
		Sociotechnical and cultural approach to management
IS/IT Strategic Planning	8	IS/IT strategic planning: competitive strategies and business intelligence, link to corporate strategy
		Strategic information systems frameworks and applications: types of IS, knowledge management, decision support systems; classification of information systems
		Management of IT human resources, employee policies, agreements, contracts
		Segregation of duties
		IS/IT training and education
IS/IT Management Issues	9	Legal issues relating to the introduction of IT to the enterprise (international and country-specific)
		Intellectual property issues in cyberspace: trademarks, copyrights, patents
		Ethical issues
		Privacy
		IT governance
		IT/IS housekeeping

Figure 2—Management, Planning and Organization of IS Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
Support Tools and Frameworks	6	COBIT: *Management Guidelines,* a framework for IT/IS managers
		COBIT: audit's use in support of the business cycle
		International standards and good practices: ISOI7799, ITIL, privacy standards, COSO, COCO, Cadbury, King
Techniques	4	Change control reviews
		Operational reviews
		ISO9000 reviews
Total Hours	**37**	

Figure 3—Technical Infrastructure and Operational Practices Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
Technical Infrastructure (Planning, Implementation and Operational Practices)	25	IT architecture/standards
		Hardware: all IT equipment, including mainframe, minicomputers, client-servers, routers, switches, communications, PCs, etc.
		Software: operating systems, utility software, database systems, etc.
		Network: communications equipment and services rendered to provide networks, network-related hardware, network-related software, use of service providers that provide communication services, etc.
		Baseline controls
		Security/testing and validation
		Performance monitoring and evaluation tools
		IT governance: maintaining and making it work for IT
		IT control monitoring and evaluation tools, such as access control systems monitoring or intrusion detection systems monitoring
		Managing information resources and information infrastructure: enterprise management software
		Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799
		Issues and considerations of service center vs. proprietary technical infrastructures
		Open systems
Service Center Management: Maintain Information Systems and Technical Infrastructures Through Organizations Dedicated to These Activities	12	Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799
		Change management/implementation of new and changed systems: organization of the tools used to control the introduction of new and changed products into the service center environment
		Security management
		Resource/configuration management: compliance with organization/IT operating standards, policies and procedures (i.e., proper use of computer languages)
		Problem and incident management
		Capacity planning and prognosis
		Management of the distribution of automated systems
		Administration of release and versions of automated systems
		Management of suppliers
		Customer liaison
		Service level management
		Contingency/backup and recovery management
		Call center management
		Management of operations of the infrastructure (central and distributed)
		Network management
		Risk management
		Key management principles
Total Hours	**37**	

Figure 4—Protection of Information Assets Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
Information Assets Security Management	8	Information technology and security basics, concept of IT security, need for securing IT resources, policy framework on IT assets security, management of IT security, training
		Standards, compliance and assurance on IT security
Logical IT Security	9	Components of logical IT security, logical access control issues and exposures, access control software
		Logical security risks, controls and audit considerations (audit of logical access, security testing)
		Logical security features, tools, procedures
Applied IT Security: High-technology Resources	9	Communications and network security: principles of network security, client-server, Internet and web-based services, firewall security systems and other connectivity protection resources (e.g., cryptography, digital signatures, key management policies), intrusion detections systems, COBIT, system reviews
		Mainframe security facilities
		Basic database application and system security
		Security in the system development and maintenance processes
Physical and Environmental Security	3	Environmental issues and exposures: concepts on physical IT security
		Physical access exposures and controls
Total Hours	**29**	

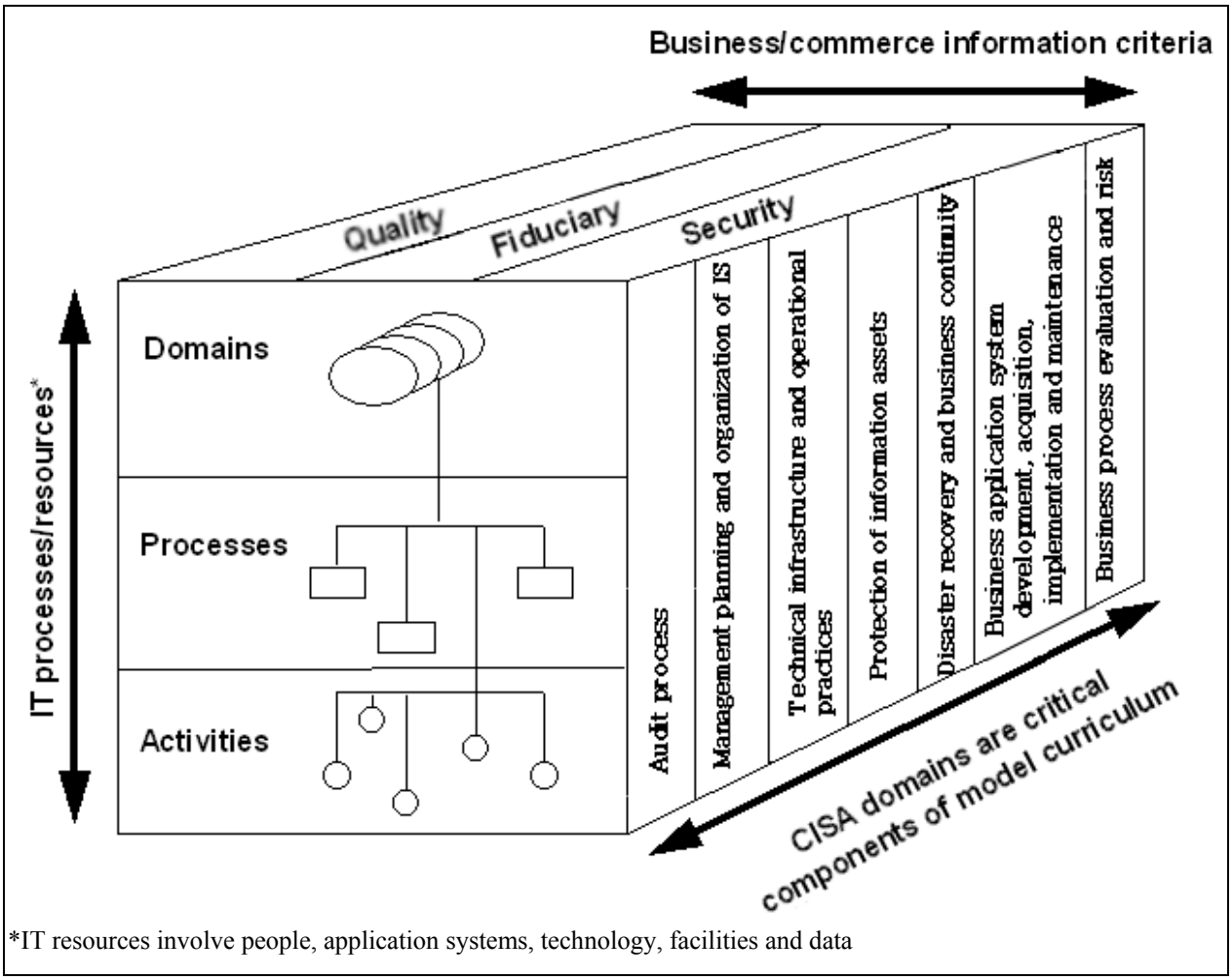
Figure 5—Disaster Recovery and Business Continuity Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning	10	Management support and commitment to the process
		Plan preparation and documentation
		Management approval and distribution of the plan
		Testing, maintenance and revision of the plan; training
		Audit's role
		Backup provisions
		Business continuity planning
		Business impact analysis
Insurance	2	Description of insurance
		Items that can be insured
		Types of insurance coverage
		Valuation of assets: equipment, people, information process, technology
Total Hours	**12**	

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
IS Planning	9	IS managing components (e.g., data processes, technologies, organization), understanding stakeholders and their requirements
		IS planning methods: system investigation, process integration/reengineering opportunities, risk evaluation, cost-benefit analysis, risk assessment, object-oriented systems analysis and design
		ERP software enterprise applications integration
Information Management and Usage	16	Monitoring service-level performance against service level agreements, quality of service, availability, response time, security and controls, processing integrity, privacy, remedies, amending SLAs
		Data and information: analyze, evaluate and design information architecture (i.e., the role of databases and database management systems, including knowledge management systems and data warehouses)
		Data and application architecture (e.g., IS modeling, business models, processes and solutions); analysis, evaluations and design of an entity's business processes and business models
		Information management (data administration, database functions and administration, database administrator roles and responsibilities)
		Database technology as tools for the auditor
		Data structures and basic SQL language
Develop-ment, Acquisition and Maintenance of Information Systems	12	Information systems project management: planning, organization, human resource deployment, project control, monitoring, execution
		Traditional methods for the system development life cycle (SDLC); analysis, evaluation and design of an entity's SDLC phases and tasks
		Approaches for system development: software packages, prototyping, business process reengineering, computer aided software engineering (CASE) tools
		System maintenance and change control procedures for system changes
		Risk and control issues, analysis and evaluation of project characteristics and risks
Impact of IT on the Business Processes and Solutions	4	Business process outsourcing (BPO)
		Applications of e-business issues and trends
Software Development	11	Separation of specification and implementation in programming
		Requirements specification methodology
		Algorithm design, sorting and searching algorithms
		File handling
		Linked lists and binary trees
		Database creation and manipulation
		Principles of good screen and report design
		Program language alignment
Total Hours	**52**	

Figure 7—Business Process Evaluation and Risk Management Domain ISACA Model Curriculum		
Topics	**Hours**	**Subtopics**
Audit and Development of Application Controls	19	Input/origination controls
		Processing control procedures
		Output controls
		Application system documentation
		Audit trails
Total Hours	**19**	

Appendix 1. Relevance of ISACA Model Curriculum to COBIT Conceptual Framework and CISA Content Areas

Figure 8—Relevance of ISACA Model Curriculum to COBIT Conceptual Framework and CISA Content Areas



*IT resources involve people, application systems, technology, facilities and data

The topics in the ISACA model curriculum are designed to provide professional entry level skills and capabilities in business/commerce areas. The seven CISA content areas (domains) and their subtopics were used to provide a structure to organize the issues in the ISACA model curriculum. IT processes are addressed by COBIT, which is integrated into the CISA content areas (**figure 8**).

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.

Managerial Communications and/or Public Speaking

These are communication skills that are employed when discussing audit scope, findings and recommendations.

Interviewing Skills

This includes the effective gathering of information when interviewing management and completing control questionnaires.

Negotiation Skills and/or Personal Selling

This is needed to convince management to implement recommendations for positive change.

Business Writing

This is useful to produce understandable and usable reports and other written communications.

Industrial Psychology and/or Behavioral Science

This includes the ability to understand and effectively manage human behavior throughout the audit process.

Project Management/Time Budgeting

This includes the essential ability to effectively and efficiently manage time and tasks during audits. Auditors are frequently evaluated on meeting budgets.

Team Building and Team Leading

This includes effectively managing team activities with proper coordination and utilization of knowledge and skills of individual team members in the performance of an IS audit.

Appendix 3. Compliance Grid for the *ISACA Model Curriculum for IS Audit and Control*

To map a program to the *ISACA Model Curriculum for IS Audit and Control*, 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 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 compliance with the model, the total time spent in hours should be at least 244 hours and all areas in the model should have reasonable coverage. Note: 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, looking at the model matrix on one and the syllabus/expanded course outline on the other, facilitates the process.

The mapping process steps are listed in **figure 9**.

Figure 9—Mapping Process Steps	
1	Identify all direct and support courses that apply to the program.
2	Make sure 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. Literally 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 the subject was covered based on the syllabus.
5	If unsure 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.

Submit the completed tables to ISACA for review by e-mail, *research@isaca.org*, fax +1.847.253.1443, or mail to the attention of the director of research, standards and academic relations at ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA. If the program is found to be in compliance 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 Certified Information System Auditor (CISA) certification.

Figure 1—Audit Process Domain Compliance Grid				
Topic	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
IS Audit Function Knowledge	6	Laws and regulations: audit charter		
		Nature of audit: demand for audits (e.g., agency theory, insurance hypothesis, information hypothesis)		
		Nature of IS audit: need for control and audit of computer-based IS		
		Types of audit and auditor: IS, external, internal, government/public sector		
		IS auditor responsibility, authority, and accountability: audit charter, outsourcing of IS audit activities		
		Regulation and control of IS audit: ISACA standards, guidelines, Code of Professional Ethics; laws; regulations		
Fundamental Auditing Concepts	7	Materiality: application of materiality for IS audit compared to materiality for financial statement auditing		
		Evidence: types of evidence; meaning of sufficient, reliable, relevant evidence		
		Independence: need for independence in attitude and appearance, situations that may impair independence		
		Audit risk: inherent risk, control risk, detection risk		
		IS and general audit responsibilities for fraud		
		Assurance		
Standards and Guidelines for IS Auditing	5	Knowledge of ISACA Code of Professional Ethics		
		Review of current ISACA IS Auditing Standards and Guidelines		
		Standards and guidelines specific to a region/country: ACM, AGA, AICPA, AITP, IFAC, IIA, ISO, NIA		
		IS audit practices and techniques		
Internal Controls Concepts Knowledge	13	Relevance, structure and indicators of effective IT governance for organizations and IS auditors; IT governance structure		
		Internal control objectives; internal control and documentation of IS, COCO, COSO, King, Sarbanes-Oxley Act of 2002, SAS94		
		Control classifications: preventive, detective, compensating/corrective		

Figure 1—Audit Process Domain Compliance Grid				
Topic	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Iternal Controls Concepts Knowledge continued		General controls: organizational, security, general operating and disaster recovery, development, documentation		
		Application controls: control objectives; classifications of application controls, e.g., computerized/manual, input/processing/output, preventive/detective/corrective, audit trails		
		COBIT: Structure and relevance of COBIT for organizations and IS auditors		
Audit Planning Process	7	Strategic/tactical audit planning		
		Engagement letter: purpose and content of engagement letters		
		Risk assessment: risk-based auditing; risk assessment methods; standards: AS-NZ 4360, CRAMM		
		Preliminary evaluation of internal controls: information gathering and control evaluation techniques		
		Audit plan, program and scope: compliance vs. substantive testing, application of risk assessment to audit plan		
		Classification, scope of audits: e.g., financial, operational, general, application, OS, physical, logical		
Audit Management	5	Resource allocation/prioritization/planning/ execution/reassignments		
		Evaluating audit quality/peer reviews		
		Best practice identification		
		Computer information systems (CIS) audit career development		
		Career path planning		
		Performance assessment		
		Performance counseling and feedback		
		Training (internal/external)		
		Professional development (certifications, professional involvement, etc.)		
Audit Evidence Process	12	Evidence: sufficient, reliable, relevant, useful		
		Evidence gathering techniques, e.g., observation, inquiry, interview, testing		
		Compliance vs. substantive testing: nature of and difference between compliance and substantive testing, types of compliance test, types of substantive test		
		Sampling: sampling concepts, statistical and nonstatistical approaches, design and selection of samples, evaluation of sample results		
		Computer-assisted audit techniques (CAATs): need for, types of, planning for and using CAATs; continuous online auditing approach		

Figure 1—Audit Process Domain Compliance Grid				
Topic	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Audit Evidence Process continued		Documentation: relationship with audit evidence; uses of documentation; minimum content; custody, retention, retrieval		
		Analysis: judge the materiality of findings, identify reportable conditions, reach conclusions		
		Review: provide reasonable assurance that objectives have been achieved		
Audit Reporting Follow-up	3	Form and content of audit report: purpose, structure and content, style, intended recipient, type of opinion, consideration of subsequent events		
		Management actions to implement recommendations		
Total Hours	**58**			

Figure 2—Management, Planning and Organization of IS Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
IS/IT Management	10	IT project management		
		Risk management: economic, social, cultural, technology risk management		
		Software quality control management		
		Management of IT infrastructure and alternative IT architectures, configuration management		
		Management of IT delivery (operations) and support (maintenance)		
		Performance measurement and reporting: IT balanced scorecard		
		Outsourcing		
		Quality assurance		
		Sociotechnical and cultural approach to management		
IS/IT Strategic Planning	8	IS/IT strategic planning: competitive strategies and business intelligence, link to corporate strategy		
		Strategic information systems frameworks and applications: types of IS, knowledge management, decision support systems; classification of information systems		
		Management of IT human resources, employee policies, agreements, contracts		
		Segregation of duties		
		IS/IT training and education		
IS/IT Management Issues	9	Legal issues relating to the introduction of IT to the enterprise (international and country-specific)		
		Intellectual property issues in cyberspace: trademarks, copyrights, patents		
		Ethical issues		
		Privacy		
		IT governance		
		IT/IS housekeeping		

Figure 2—Management, Planning and Organization of IS Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Support Tools and Frameworks	6	COBIT: *Management Guidelines*, a framework for IT/IS managers		
		COBIT: audit's use in support of the business cycle		
		International standards: ISOI7799, privacy standards, COCO, COSO, Cadbury, King, ITIL		
Techniques	4	Change control reviews		
		Operational reviews		
		ISO9000 reviews		
Total Hours	**37**			

Figure 3—Technical Infrastructure and Operational Practices Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Technical Infrastructure (Planning, Implementation and Operational Practices)	25	IT architecture/standards		
		Hardware: all IT equipment, including mainframe, minicomputers, client-servers, routers, switches, communications, PCs, etc.		
		Software: operating systems, utility software, database systems, etc.		
		Network: communications equipment and services rendered to provide networks, network-related hardware, network-related software, use of service providers that provide communication services, etc.		
		Baseline controls		
		Security/testing and validation		
		Performance monitoring and evaluation tools		
		IT governance: maintaining it and making it work for IT		
		IT control monitoring and evaluation tools, such as access control systems monitoring or intrusion detection systems monitoring		
		Managing information resources and information infrastructure: enterprise management software		
		Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799		
		Issues and considerations of service center vs. proprietary technical infrastructures		
		Open systems		
Service Center Management: Maintain Information Systems and Technical Infrastructures Through Organizations	12	Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799		
		Change management/implementation of new and changed systems: organization of the tools used to control the introduction of new and changed products into the service center environment		
		Security management		

Figure 3—Technical Infrastructure and Operational Practices Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Dedicated to These Activities		Resource/configuration management: compliance with organization/IT operating standards, policies and procedures (i.e., proper use of computer languages)		
		Problem and incident management		
		Capacity planning and prognosis		
		Management of the distribution of automated systems		
		Administration of release and versions of automated systems		
		Management of suppliers		
		Customer liaison		
		Service level management		
		Contingency/backup and recovery management		
		Call center management		
		Management of operations of the infrastructure (central and distributed)		
		Network management		
		Risk management		
		Key management principles		
Total Hours	**37**			

Figure 4—Protection of Information Assets Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Information Assets Security Management	8	Information technology and security basics, concept of IT security, need for securing IT resources, policy framework on IT assets security, management of IT security, training		
		Standards, compliance and assurance on IT security		
Logical IT Security	9	Components of logical IT security, logical access control issues and exposures, access control software		
		Logical security risks, controls and audit considerations (audit of logical access, security testing)		
		Logical security features, tools, procedures		
Applied IT Security: High-technology Resources	9	Communications and network security: principles of network security, client-server, Internet and web-based services, firewall security systems and other connectivity protection resources (e.g., cryptography, digital signatures, key management policies), intrusion detections systems, COBIT, system reviews		
		Mainframe security facilities		
		Basic database application and system security		
		Security in the system development and maintenance processes		

Figure 4—Protection of Information Assets Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Physical and Environmental Security	3	Environmental issues and exposures: concepts on physical IT security		
		Physical access exposures and controls		
Total Hours	**29**			

Figure 5—Disaster Recovery and Business Continuity Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning	10	Management support and commitment to the process		
		Plan preparation and documentation		
		Management approval and distribution of the plan		
		Testing, maintenance and revision of the plan; training		
		Audit's role		
		Backup provisions		
		Business continuity planning		
		Business impact analysis		
Insurance	2	Description of insurance		
		Items that can be insured		
		Types of insurance coverage		
		Valuation of assets: equipment, people, information process, technology		
Total Hours	**12**			

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
IS Planning	9	IS managing components (e.g., data processes, technologies, organization), understanding stakeholders and their requirements		
		IS planning methods: system investigation, process integration/reengineering opportunities, risk evaluation, cost-benefit analysis, risk assessment, object-oriented systems analysis and design		
		ERP software enterprise applications integration		
Information Management and Usage	16	Monitoring service level performance against service level agreements, quality of service, availability, response time, security and controls, processing integrity, privacy, remedies, amending SLAs		
		Data and information: analyze, evaluate and design information architecture (i.e., the role of databases and database management systems, including knowledge management systems and data warehouses)		
		Data and application architecture (e.g., IS modeling, business models, processes and solutions); analysis, evaluation and design of an entity's business processes and business		

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
		models		
		Information management (data administration, database functions and administration, DBA roles and responsibilities)		
		Database technology as tools for the auditor		
Development, Acquisition and Maintenance of Information Systems	12	Information systems project management: planning, organization, human resource deployment, project control, monitoring, execution		
		Traditional methods for the system development life cycle (SDLC); analysis, evaluation and design of an entity's SDLC phases and tasks		
		Approaches for system development: software packages, prototyping, business process reengineering, computer aided software engineering (CASE) tools		
		System maintenance and change control procedures for system changes		
		Risk and control issues, analysis and evaluation of project characteristics and risks		
Impact of IT on the Business Processes and Solutions	4	Business process outsourcing (BPO)		
		Applications of e-business issues and trends		
Software Development	11	Separation of specification and implementation in programming		
		Requirements specification methodology		
		Algorithm design, sorting and searching algorithms		
		File handling		
		Linked lists and binary trees		
		Database creation and manipulation		
		Principles of good screen and report design		
		Program language alignment		
Total Hours	**52**			

Figure 7—Business Process Evaluation and Risk Management Domain Compliance Grid				
Topics	**Hrs**	**Subtopics**	**Course(s) Covering Topic**	**Hours**
Audit and Development of Application Controls	19	Input/origination controls		
		Processing control procedures		
		Output controls		
		Application system documentation		
		Audit trails		
Total Hours	**19**			

Grand Total	**244**	**Total hours figures 1 through 7 compliance grid**		

Appendix 4. Examples of Mapping Programs to the ISACA Model Curriculum Compliance Grid

Bowling Green State University (BGSU), USA, Undergraduate IS Audit Degree Program Compliance Grid for the Model Curriculum

Figure 1—Audit Process Domain (BGSU)				
Subtopic	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
IS Audit Function Knowledge	6	Laws and regulations: audit charter	Acct 460 Accounting Information Systems Acct 451 Auditing I Acct 456 Information Systems Auditing and Control	1 5 1
		Nature of audit: demand for audits (e.g., agency theory, insurance hypothesis, information hypothesis)		
		Nature of IS audit: need for control and audit of computer-based IS		
		Types of audit and auditor: IS, external, internal, government/public sector		
		IS auditor responsibility, authority, and accountability: audit charter, outsourcing of IS audit activities		
		Regulation and control of IS audit: ISACA standards, guidelines, Code of Professional Ethics; laws; regulations		
Fundamental Auditing Concepts	7	Materiality: application of materiality for IS audit compared to materiality for financial statement audit	Acct 460 Accounting Information Systems Acct 451 Auditing I	9 1
		Evidence: types of evidence; meaning of sufficient, reliable, relevant evidence		
		Independence: need for independence in attitude and appearance, situations that may impair independence		
		Audit risk: inherent risk, control risk, detection risk		
		IS and general audit responsibilities for fraud		
		Assurance		
Standards and Guidelines for IS Auditing	5	Knowledge of ISACA Code of Professional Ethics	Acct 460 Accounting Information Systems Acct 451 Auditing I Acct 456 Information Systems Auditing and Control	1 1 2
		Review of current ISACA IS Auditing Standards and Guidelines		
		Standards and guidelines specific to a region/country: ACM, AGA, AICPA, AITP, IFAC, IIA, ISO, NIA		
		IS auditing practices and techniques		
Internal Controls Concepts Knowledge	13	Relevance, structure and indicators of effective IT governance for organizations and IS auditors; IT governance structure	Acct 460 Accounting Information Systems Acct 451 Auditing I MIS 471 Systems Analysis and Design	6 2 6
		Internal control objectives; internal control and documentation of IS, COSO, COCO, King, Sarbanes-Oxley Act of 2002, SAS94		
		Control classifications: preventive, detective, compensating/corrective		
		General controls: organizational, security, general operating and disaster recovery, development, documentation		

Figure 1—Audit Process Domain (BGSU)				
Subtopic	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Internal Controls Concepts Knowledge continued		Application controls: control objectives; classifications of application controls, e.g., computerized/manual, input/processing/output, preventive/detective/corrective, audit trails		
		COBIT: Structure and relevance of COBIT for organizations and IS auditors		
Audit Planning Process	7	Strategic/tactical audit planning	Acct 451 Auditing I Acct 456 Information Systems Auditing and Control	7 1
		Engagement letter: purpose and content of engagement letters		
		Risk assessment: risk-based auditing, risk assessment methods, standards: AS-NZ 4360, CRAMM		
		Preliminary evaluation of internal controls: information gathering and control evaluation techniques		
		Audit plan, program and scope: compliance vs. substantive testing, application of risk assessment to audit plan		
		Classification, scope of audits: e.g., financial, operational, general, application, OS, physical, logical		
Audit Management	5	Resource allocation/prioritization/planning/ execution/reassignments	Acct 451 Auditing I	2
		Evaluating audit quality/peer reviews		
		Best practice identification		
		Computer information systems (CIS) audit career development		
		Career path planning		
		Performance assessment		
		Performance counseling and feedback		
		Training (internal/external)		
		Professional development (certifications, professional involvement, etc.)		
Audit Evidence Process	12	Evidence: sufficient, reliable, relevant, useful	Acct 460 Accounting Information Systems Acct 451 Auditing I	3 10
		Evidence gathering techniques, e.g., observation, inquiry, interview, testing		
		Compliance vs. substantive testing: nature of and difference between compliance and substantive testing, types of compliance test, types of substantive test		
		Sampling: sampling concepts, statistical and nonstatistical approaches, design and selection of samples, evaluation of sample results		
		Computer-assisted audit techniques (CAATs): need for, types of, planning for and using CAATs; continuous online auditing approach		
		Documentation: relationship with audit evidence; uses of documentation; minimum content; custody, retention, retrieval		

Figure 1—Audit Process Domain (BGSU)				
Subtopic	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Audit Evidence Process continued		Analysis: judge the materiality of findings, identify reportable conditions, reach conclusions		
		Review: provide reasonable assurance that objectives have been achieved		
Audit Reporting Follow-up	3	Form and content of audit report: purpose, structure and content, style, intended recipient, type of opinion, consideration of subsequent events	Acct 451 Auditing I	4
		Management actions to implement recommendations		
Total Hours	**58**		**Total**	**62**

Figure 2—Management, Planning and Organization of IS Domains (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
IS/IT Management	10	IT project management	MIS 421 Business Data Communication and Distributed Processing MIS 471 Systems Analysis and Design Acct 456 Information Systems Auditing and Control	1 9 1
		Risk management: economic, social, cultural, technology risk management		
		Software quality control management		
		Management of IT infrastructure and alternative IT architectures, configuration management		
		Management of IT delivery (operations) and support (maintenance)		
		Performance measurement and reporting: IT balanced scorecard		
		Outsourcing		
		Quality assurance		
		Sociotechnical and cultural approach to management		
IS/IT Strategic Planning	8	IS/IT strategic planning: competitive strategies and business intelligence, link to corporate strategy	MIS 200 Introduction to Management Information Systems Acct 460 Accounting Information Systems MIS 421 Business Data Communication and Distributed Processing Acct 456 Information Systems Auditing and Control	2 1 2 2
		Strategic information systems frameworks and applications: types of IS, knowledge management, decision support systems; classification of information systems		
		Management of IT human resources, employee policies, agreements, contracts		
		Segregation of duties		
		IS/IT training and education		
IS/IT Management Issues	9	Legal issues relating to the introduction of IT to the enterprise (international and country-specific)	MIS 200 Introduction to Management Information Systems Acct 460 Accounting Information Systems MIS 471 Systems Analysis and Design Acct 456 Information Systems Auditing and Control	1 1 6 1
		Intellectual property issues in cyberspace: trademarks, copyrights, patents		
		Ethical issues		
		Privacy		
		IT governance		
		IT/IS housekeeping		

Figure 2—Management, Planning and Organization of IS Domains (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Support Tools and Frameworks	6	COBIT: *Management Guidelines*, a framework for IT/IS managers	Acct 460 Accounting Information Systems	1
		COBIT: audit's use in support of the business cycle	Acct 456 Information Systems Auditing and Control	1
		International standards and good practices: ISOI7799, ITIL, privacy standards, COCO, COSO, Cadbury, King		
Techniques	4	Change control reviews	Acct 456 Information Systems Auditing and Control	3
		Operational reviews		
		ISO9000 reviews		
Total Hours	**37**		**Total**	**32**

Figure 3—Technical Infrastructure and Operational Practices Domains (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Technical Infrastructure (Planning, Implementation and Operational Practices)	25	IT architecture/standards	MIS 200 Introduction to Management Information Systems	3
		Hardware: all IT equipment, including mainframe, minicomputers, client-servers, routers, switches, communications, PCs, etc.	Acct 460 Accounting Information Systems	3
		Software: operating systems, utility software, database systems, etc.	MIS 421 Business Data Communication and Distributed Processing	27
		Network: communications equipment and services rendered to provide networks, network-related hardware, network-related software, use of service providers that provide communication services, etc.		
		Baseline controls		
		Security/testing and validation		
		Performance monitoring and evaluation tools		
		IT governance: maintaining it and making it work for IT		
		IT control monitoring and evaluation tools, such as access control systems monitoring or intrusion detection systems monitoring		
		Managing information resources and information infrastructure: enterprise management software		
		Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799		
		Issues and considerations of service center vs. proprietary technical infrastructures		
		Open systems		
Service Center Management: Maintain Information Systems and Technical Infrastruc-	12	Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799	Acct 460 Accounting Information Systems	1
		Change management/implementation of new and changed systems: organization of the tools used to control the introduction of new and changed products into the service center environment	MIS 471 Systems Analysis and Design	3
		Security management	Acct 456 Information Systems Auditing and Control	4

Figure 3—Technical Infrastructure and Operational Practices Domains (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
tures Through Organiza-tions Dedicated to These Activities		Resource/configuration management: compliance with organization/IT operating standards, policies and procedures (i.e., proper use of computer languages)		
		Problem and incident management		
		Capacity planning and prognosis		
		Management of the distribution of automated systems		
		Administration of release and versions of automated systems		
		Management of suppliers		
		Customer liaison		
		Service level management		
		Contingency/backup and recovery management		
		Call center management		
		Management of operations of the infrastructure (central and distributed)		
		Network management		
		Risk management		
		Key management principles		
Total Hours	**37**		**Total**	**41**

Figure 4—Protection of Information Assets Domain (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Information Assets Security Management	8	Information technology and security basics, concept of IT security, need for securing IT resources, policy framework on IT assets security, management of IT security, training	MIS 200 Introduction to Management Information Systems	2
		Standards, compliance and assurance on IT security	MIS 421 Business Data Communication and Distributed Processing	1
			Acct 460 Accounting Information Systems	1
			Acct 451 Auditing I	2
			Acct 456 Information Systems Auditing and Control	3
Logical IT Security	9	Components of logical IT security, logical access control issues and exposures, access control software	Acct 460 Accounting Information Systems	1
		Logical security risks, controls and audit considerations (audit of logical access, security testing)	MIS 421 Business Data Communication and Distributed Processing	1
		Logical security features, tools, procedures	MIS 471 Systems Analysis and Design	6
			Acct 456 Information Systems Auditing and Control	2
Applied IT Security: High-technology Resources	9	Communications and network security: principles of network security, client-server, Internet and web-based services, firewall security systems and other connectivity protection resources (e.g., cryptography, digital signatures, key management policies), intrusion detections systems, COBIT, system reviews	Acct 460 Accounting Information Systems	1
			MIS 421 Business Data Communication and Distributed Processing	1
			Acct 451 Auditing I	1
			Acct 456 Information Systems Auditing and Control	5

Figure 4—Protection of Information Assets Domain (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
		Mainframe security facilities		
		Basic database application and system security		
		Security in the system development and maintenance processes		
Physical and Environmental Security	3	Environmental issues and exposures: concepts on physical IT security	Acct 460 Accounting Information Systems	1
		Physical access exposures and controls	Acct 456 Information Systems Auditing and Control	1
Total Hours	**29**		**Total**	**29**

Figure 5—Disaster Recovery and Business Continuity Domain (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning	10	Management support and commitment to the process	Acct 460 Accounting Information Systems	1
		Plan preparation and documentation	MIS 421 Business Data Communication and Distributed Processing	1
		Management approval and distribution of the plan		
		Testing, maintenance and revision of the plan; training	MIS 471 Systems Analysis and Design	1
		Audit's role	Acct 456 Information Systems Auditing and Control	4
		Backup provisions		
		Business continuity planning	MIS 470 Database Management	
		Business impact analysis		1
Insurance	2	Description of insurance	Acct 456 Information Systems Auditing and Control	1
		Items that can be insured		
		Types of insurance coverage	Acct 451 Auditing I	
		Valuation of assets: equipment, people, information process, technology		1
Total Hours	**12**		**Total**	**10**

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
IS Planning	9	IS managing components (e.g., data processes, technologies, organization), understanding stakeholders and their requirements	Acct 460 Accounting Information Systems MIS 421 Business Data Communication and Distributed Processing MIS 471 Systems Analysis and Design	1 1 4
		IS planning methods: system investigation, process integration/reengineering opportunities, risk evaluation, cost-benefit analysis, risk assessment, object-oriented systems analysis and design		
		ERP software enterprise applications integration		
Information Management and Usage	16	Monitoring service level performance against service level agreements, quality of service, availability, response time, security and controls, processing integrity, privacy, remedies, amending SLAs	MIS 200 Introduction to Management Information Systems Acct 460 Accounting Information Systems MIS 421 Business Data Communication and Distributed Processing MIS 470 Database Management Acct 456 Information Systems Auditing and Control	2 6 1 3 3
		Data and information: analyze, evaluate and design information architecture (i.e., the role of databases and database management systems, including knowledge management systems and data warehouses)		
		Data and application architecture (e.g., IS modeling, business models, processes and solutions); analysis, evaluation and design of an entity's business processes and business models		
		Information management (data administration, database functions and administration, DBA roles and responsibilities)		
		Database technology as tools for the auditor		
Development, Acquisition and Maintenance of Information Systems	12	Information systems project management: planning, organization, human resource deployment, project control, monitoring, execution	MIS 200 Introduction to Management Information Systems Acct 460 Accounting Information Systems MIS 421 Business Data Communication and Distributed Processing MIS 471 Systems Analysis and Design Acct 456 Information Systems Auditing and Control	2 3 2 3 2
		Traditional methods for the system development life cycle (SDLC); analysis, evaluation and design of an entity's SDLC phases and tasks		
		Approaches for system development: software packages, prototyping, business process reengineering, compurer aided software engineering (CASE) tools		
		System maintenance and change control procedures for system changes		
		Risk and control issues, analysis and evaluation of project characteristics and risks		

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Impact of IT on the Business Processes and Solutions	4	Business process outsourcing (BPO)	MIS 200 Introduction to Management Information Systems	1
		Applications of e-business issues and trends	Acct 456 Information Systems Auditing and Control	3
Software Development	11	Separation of specification and implementation in programming	Acct 460 Accounting Information Systems	2
		Requirements specification methodology	MIS 470 Database Management	12
		Algorithm design, sorting and searching algorithms		
		File handling		
		Linked lists and binary trees		
		Database creation and manipulation		
		Principles of good screen and report design		
		Program language alignment		
Total Hours	**52**		**Total**	**51**

Figure 7—Business Process Evaluation and Risk Management Domain (BGSU)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Audit and Development of Application Controls	19	Input/origination controls	Acct 460 Accounting Information Systems	1
		Processing control procedures		
		Output controls	Acct 451 Auditing I	1
		Application system documentation	MIS 471 Systems Analysis and Design	12
		Audit trails		
			Acct 456 Information Systems Auditing and Control	5
Total Hours	**19**		**Total**	**19**

Grand Total	**244**	**Total hours figures 1 through 7 BGSU**	**Bowling Green State University Grand Total**	**244**

Bowling Green State University (BGSU) has a specialization within its Bachelor of Science in Business Administration (BSBA) degree program titled Information Systems Auditing and Control (ISAC). The example presented herein refers to courses within the BSBA degree program. BGSU also has a Master of Accountancy (MAcc) degree program that requires the equivalent of a bachelor's degree in accounting prior to entry into the program. The MAcc degree program has a track titled ISAC, which provides the coursework to complement a bachelor in accounting program to meet the ISACA model curriculum requirements. The course names and numbers slightly differ in the MAcc program from the names and numbers in the BSBA, but the course topic coverage is comparable. Both the BSBA and MAcc programs that focus on ISAC require coursework about topics that are not addressed in the ISACA model curriculum. Many of these topics are similar to those presented in Appendix 2, Suggested Supplemental Skills for IS Auditors.

Comment Summary

- One hour to complete the grid per instructor times six instructors plus six hours to coordinate and summarize, equals 12 total hours spent to map the program.
- Hours are for major topics with additional descriptions for subtopics. Hour estimates are required only at the major topic level.
- The format allows for a wide differentiation in programs that still follow the model curriculum.
- Topics such as ethics may be stressed throughout the program but may not ever be discussed as an ethics lecture.
- Since many of the courses are not designed exclusively for the ISACA program, there may be wide fluctuations in the course content from one instructor to another and from one semester to another.

California State Polytechnic University, USA, MSBA-IS Audit Graduate Program Compliance Grid for the Model Curriculum

Figure 1—Audit Process Domain (Cal State)				
Subtopic	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
IS Audit Function Knowledge	6	Laws and regulations: audit charter	CIS 433 CIS Auditing GBA 560 Legal Environment of Information Systems GBA 577 Advanced IT Auditing	2 4 2
		Nature of audit: demand for audits (e.g., agency theory, insurance hypothesis, information hypothesis)		
		Nature of IS audit: need for control and audit of computer-based IS		
		Types of audit and auditor: IS, external, internal, government/public sector		
		IS auditor responsibility, authority, and accountability: audit charter, outsourcing of IS audit activities		
		Regulation and control of IS audit: ISACA standards, guidelines, Code of Professional Ethics; laws; regulations		
Fundamental Auditing Concepts	7	Materiality: application of materiality for IS audit compared to materiality for financial statement audit	CIS 433 CIS Auditing GBA 560 Legal Environment of Information Systems GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy GBA 608/609 Managerial Accounting Issues and Practices	3 3 2 2 5
		Evidence: types of evidence; meaning of sufficient, reliable, relevant evidence		
		Independence: need for independence in attitude and appearance, situations that may impair independence		
		Audit risk: inherent risk, control risk, detection risk		
		IS and general audit responsibilities for fraud		
		Assurance		
Standards and Guidelines for IS Auditing	5	Knowledge of ISACA Code of Professional Ethics	CIS 433 CIS Auditing GBA 560 Legal Environment of Information Systems GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy GBA 608/609 Managerial Accounting Issues and Practices	2 1 2 1 4
		Review of current ISACA IS Auditing Standards and Guidelines		
		Standards and guidelines specific to a region/country: ACM, AGA, AICPA, AITP, IFAC, IIA, ISO, NIA		
		IS audit practices and techniques		
Internal Controls Concepts Knowledge	13	Relevance, structure and indicators of effective IT governance for organizations and IS auditors; IT governance structure	CIS 433 CIS Auditing GBA554 Client-server Computing GBA 577 Computer Based Data Communications GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy GBA 608/609 Managerial Accounting Issues and	3 1 2 3
		Internal control objectives; internal control and documentation of IS, COCO, COSO, King, Sarbanes-Oxley Act of 2002, SAS94		
		Control classifications: preventive, detective, compensating/corrective		
		General controls: organizational, security, general operating and disaster recovery, development, documentation		

Figure 1—Audit Process Domain (Cal State)				
Subtopic	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
		Application controls: control objectives; classifications of application controls, e.g., computerized/manual, input/processing/output, preventive/detective/corrective, audit trails	Practices	4
		COBIT: Structure and relevance of COBIT for organizations and IS auditors		4
Audit Planning Process	7	Strategic/tactical audit planning	CIS 433 CIS Auditing GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy GBA 608/609 Managerial Accounting Issues and practices	3
		Engagement letter: purpose and content of engagement letters		3
		Risk assessment: risk-based auditing, risk assessment methods, standards: AS-NZ 4360, CRAMM		3
		Preliminary evaluation of internal controls: information gathering and control evaluation techniques		
		Audit plan, program and scope: compliance vs. substantive testing, application of risk assessment to audit plan		4
		Classification, scope of audits: e.g., financial, operational, general, application, OS, physical, logical		
Audit Management	5	Resource allocation/prioritization/planning/ execution/reassignments	CIS 433 CIS Auditing GBA 577 Advanced IT Auditing BA 578 Information Security and Privacy GBA 608/609 Managerial Accounting Issues and Practices	2
		Evaluating audit quality/peer reviews		3
		Best practice identification		
		Computer information systems (CIS) audit career development		2
		Career path planning		
		Performance assessment		
		Performance counseling and feedback		3
		Training (internal/external)		
		Professional development (certifications, professional involvement, etc.)		
Audit Evidence Process	12	Evidence: sufficient, reliable, relevant, useful	CIS 433 CIS Auditing GBA 560 Legal Environment of Information Systems GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy	2
		Evidence gathering techniques, e.g., observation, inquiry, interview, testing		8
		Compliance vs. substantive testing: nature of and difference between compliance and substantive testing, types of compliance test, types of substantive test		2
		Sampling: sampling concepts, statistical and nonstatistical approaches, design and selection of samples, evaluation of sample results		1
		Computer-assisted audit techniques (CAATs): need for, types of, planning for and using CAATs; continuous online auditing approach		
		Documentation: relationship with audit evidence; uses of documentation; minimum content; custody, retention, retrieval		

Figure 1—Audit Process Domain (Cal State)				
Subtopic	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
		Analysis: judge the materiality of findings, identify reportable conditions, reach conclusions		
		Review: provide reasonable assurance that objectives have been achieved		
Audit Reporting Follow-up	3	Form and content of audit report: purpose, structure and content, style, intended recipient, type of opinion, consideration of subsequent events	CIS 433 CIS Auditing GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy	2 1 1
		Management actions to implement recommendations		
Total Hours	**58**		**Total**	**90**

Figure 2—Management, Planning and Organization of IS Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
IS/IT Management	10	IT project management	GBA 673/674 Management Information Systems Seminar CIS 433 CIS Auditing GBA 577 Advanced IT Auditing GBA 557 Computer-Based Data Communications GBA 554 Client-server Computing	6 1 1 2 3
		Risk management: economic, social, cultural, technology risk management		
		Software quality control management		
		Management of IT infrastructure and alternative IT architectures, configuration management		
		Management of IT delivery (operations) and support (maintenance)		
		Performance measurement and reporting: IT balanced scorecard		
		Outsourcing		
		Quality assurance		
		Sociotechnical and cultural approach to management		
IS/IT Strategic Planning	8	IS/IT strategic planning: competitive strategies and business intelligence, link to corporate strategy	GBA 673/674 Management Information Systems Seminar GBA 557 Computer-based Data Communications CIS 433 CIS Auditing GBA 577 Advanced IT Auditing	6 4 1 1
		Strategic information systems frameworks and applications: types of IS, knowledge management, decision support systems; classification of information systems		
		Management of IT human resources, employee policies, agreements, contracts		
		Segregation of duties		
		IS/IT training and education		
IS/IT Management Issues	9	Legal issues relating to the introduction of IT to the enterprise (international and country-specific)	GBA 673/674 Management Information Systems Seminar GBA 560 Legal Environment of Information Systems CIS 433 CIS Auditing GBA 578 Information Systems Security and Privacy GBA 577 Advanced IT	3 8 1 3 1
		Intellectual property issues in cyberspace: trademarks, copyrights, patents		
		Ethical issues		
		Privacy		
		IT governance		

Figure 2—Management, Planning and Organization of IS Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
		IT/IS housekeeping	Auditing GBA 554 Client-server Computing GBA 557 Computer-based Data Communication	1 1
Support Tools and Frameworks	6	COBIT: *Management Guidelines*, a framework for IT/IS managers COBIT: audit's use in support of the business cycle International standards: ISOI7799, ITIL, privacy standards, COCO, COSO, Cadbury, King	CIS 433 CIS Auditing GBA 560 Legal Environment of Information Systems GBA 557 Computer-based Data Communications GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy GBA 673/674 Management Information Systems Seminar	2 2 2 2 2
Techniques	4	Change control reviews Operational reviews ISO9000 reviews	GBA 673/674 Management Information Systems Seminar GBA 577 Advanced IT Auditing CIS 433 CIS Auditing GBA 554 Client-server Computing GBA 557 Computer-based Data Communications	2 1 1 1 1
Total Hours	**37**		**Total**	**61**

Figure 3—Technical Infrastructure and Operational Practices Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Technical Infrastructure (Planning, Implement-ation and Operational Practices)	25	IT architecture/standards Hardware: all IT equipment, including mainframe, minicomputers, client/servers, routers, switches, communications, PCs, etc. Software: operating systems, utility software, database systems, etc. Network: communications equipment and services rendered to provide networks, network-related hardware, network-related software, use of service providers that provide communication services, etc. Baseline controls Security/testing and validation Performance monitoring and evaluation tools IT governance: maintaining it and making it work for IT IT control monitoring and evaluation tools, such as access control systems monitoring or intrusion detection systems monitoring	GBA 557 Computer-based Data Communications GBA 554 Client-server Computing GBA 673/674 Management Information Systems Seminar CIS 433 CIS Auditing GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy	7 8 6 2 2 2

Figure 3—Technical Infrastructure and Operational Practices Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
		Managing information resources and information infrastructure: enterprise management software		
		Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799		
		Issues and considerations of service center vs. proprietary technical infrastructures		
		Open systems		
Service Center Management: Maintain Information Systems and Technical Infrastruc-tures Through Organizations Dedicated to These Activities	12	Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799	GBA 673/674 Management Information Systems Seminar GBA 554 Client-server Computing GBA 557 Computer-based Data Communications GBA 577 Advanced IT Auditing CIS 433 CIS Auditing GBA 578 Information Systems Security and Privacy	4 5 6 2 2 2
		Change management/implementation of new and changed systems: organization of the tools used to control the introduction of new and changed products into the service center environment		
		Security management		
		Resource/configuration management: compliance with organization/IT operating standards, policies and procedures (i.e., proper use of computer languages)		
		Problem and incident management		
		Capacity planning and prognosis		
		Management of the distribution of automated systems		
		Administration of release and versions of automated systems		
		Management of suppliers		
		Customer liaison		
		Service level management		
		Contingency/backup and recovery management		
		Call center management		
		Management of operations of the infrastructure (central and distributed)		
		Network management		
		Risk management		
		Key management principles		
Total Hours	**37**		**Total**	**48**

Figure 4—Protection of Information Assets Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Information Assets Security Management	8	Information technology and security basics, concept for IT security, need for securing IT resources, policy framework on IT assets security, management of IT security, training	CIS 433 CIS Auditing GBA 560 Legal Environment of IS GBA 577 Advanced IT Auditing GBA 578 IS Security and Privacy GBA 673/674 MIS Seminar	1 1 2 5 2
		Standards, compliance and assurance on IT security		

Figure 4—Protection of Information Assets Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Logical IT Security	9	Components of logical IT security, logical access control issues and exposures, access control software	CIS 433 CIS Auditing GBA 554 Client-server Computing GBA 557 Computer-based Data Communications GBA 577 Advanced IT Auditing GBA 578 IS Security and Privacy	2 2 2 2 4
		Logical security risks, controls and audit considerations (audit of logical access, security testing)		
		Logical security features, tools, procedures		
Applied IT Security: High-technology Resources	9	Communications and network security: principles of network security, client-server, Internet and web-based services, firewall security systems and other connectivity protection resources (e.g., cryptography, digital signatures, key management policies), intrusion detections systems, COBIT, system reviews	CIS 433 CIS Auditing GBA 554 Client-server Computing GBA 557 Computer-based Data Communications GBA 577 Advanced IT Auditing GBA 578 Information Systems Security and Privacy	1 2 4 3 2
		Mainframe security facilities		
		Basic database application and system security		
		Security in the system development and maintenance process		
Physical and Environmental Security	3	Environmental issues and exposures: concepts on physical IT security	CIS 433 CIS Auditing GBA 554 Client-server Computing GBA 557 Computer-based Data Communications GBA 577 Advanced IT Auditing GBA 578 IS Security and Privacy GBA 673/674 Management Information Systems Seminar	2 1 1 1 2 1
		Physical access exposures and controls		
Total Hours	**29**		**Total**	**43**

Figure 5—Disaster Recovery and Business Continuity Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning	10	Management support and commitment to the process	CIS 433 CIS Auditing GBA 577 Advanced IT Auditing GBA 578 IS Security and Privacy GBA 673/674 MIS Seminar GBA 557 Computer-based Data Communications GBA 554 Client-server Computing GBA 608/609 Managerial Accounting Issues	2 2 3 4 3 2 2
		Plan preparation and documentation		
		Management approval and distribution of the plan		
		Testing, maintenance and revision of the plan; training		
		Audit's role		
		Backup provisions		
		Business continuity planning		
		Business impact analysis		
Insurance	2	Description of insurance	CIS 433 CIS Auditing GBA 560 Legal Environment of IS GBA 577 Advanced IT Auditing GBA 578 IS Security and Privacy GBA 608/609 Managerial Accounting Issues	1 3 1 2 2
		Items that can be insured		
		Types of insurance coverage		
		Valuation of assets: equipment, people, information process, technology		
Total Hours	**12**		**Total**	**27**

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
IS Planning	9	IS managing components (e.g., dataprocesses, technologies, organization); understanding stakeholders and their requirements	CIS 433 CIS Auditing GBA 673/674 Management Information Systems Seminar GBA 522 Systems Analysis and Design GBA 554 Client-server Computing	1 4 12 3
		IS planning methods: system investigation, process integration/reengineering opportunities, risk evaluation, cost-benefit analysis, risk assessment;, andobject-oriented systems analysis and design		
		ERP software enterprise applications integration		
Information Management and Usage	16	Monitoring service level performance against service level agreements, quality of service, availability, response time, security and controls, processing integrity, privacy, remedies, amending SLAs	CIS 433 CIS Auditing GBA 560 Legal Environment of Information Systems GBA 554 Client-server Computing GBA 522 Systems Analysis and Design GBA 524 Programming and Systems Implementation	1 2 3 8 8
		Data and information: analyze, evaluate and design information architecture (i.e., the role of databases and database management systems, including knowledge management systems and data warehouses)		
		Data and application architecture (e.g., IS modeling, business models, processes and solutions); analysis, evaluation and design of an entity's business processes and business models		

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
		Information management (data administration, database functions and administration, DBA roles and responsibilities)		
		Database technology as tools for the auditor		
Development, Acquisition and Maintenance of Information Systems	12	Information systems project management: planning, organization, human resource deployment, project control, monitoring, execution	CIS 433 CIS Auditing GBA 560 Legal Environment of IS GBA 557 Computer-based Data Communications GBA 554 Client-server Computing GBA 522 Systems Analysis and Design GBA 524 Programming and Systems Implementation	1 2 3 2 8 8
		Traditional methods for the system development life cycle (SDLC); analysis, evaluation and design of an entity's SDLC phases and tasks		
		Approaches for system development: software packages, prototyping, business process reengineering, computer aided software engineering (CASE) tools		
		System maintenance and change control procedures for system changes		
		Risk and control issues, analysis and evaluation of project characteristics and risks		
Impact of IT on the Business Processes and Solutions	4	Business process outsourcing (BPO)	CIS 433 CIS Auditing GBA 560 Legal Environment of IS GBA 615/616 Seminar in Organizational Behavior GBA 673/674 MIS Seminar	1 2 3 2
		Applications of e-business issues and trends		
Software Development	11	Separation of specification and implementation in programming	CIS 433 CIS Auditing GBA 554 Client-server Computing GBA 522 System Development GBA 524 Programming and Systems Implementation	1 1 8 8
		Requirements specification methodology		
		Algorithm design, sorting and searching algorithms		
		File handling		
		Linked lists and binary trees		
		Database creation and manipulation		
		Principles of good screen and report design		
		Program language alignment		
Total Hours	**52**		**Total**	**92**

Figure 7—Business Process Evaluation and Risk Management Domain (Cal State)				
Subtopics	**Hrs**	**Description**	**Courses Covering Subtopic**	**Hours**
Audit and Development of Application Controls	19	Input/origination controls Processing control procedures Output controls Application system documentation Audit trails	CIS 433 CIS Auditing GBA 577 Advanced IT Auditing GBA 557 Computer-based Data Communications GBA 554 Client-server Computing GBA 522 System Analysis and Development GBA 524 Programming and Systems Implementation	1 3 1 1 10 8
Total Hours	**19**		**Total**	**24**

Grand Total	**244**	**Total hours figures 1 through 7 Cal State**	**California State Pomona Polytechnic University Grand Total**	**384**

Courses Mapped

CIS 433 CIS Auditing (required directed elective for MSBA)	4 units 40 hours
GBA 522 Systems Development	4 units 40 hours
GBA 524 Programming and Implementation	4 units 40 hours
GBA 554 Client-server Computing (Elective)	4 units 40 hours
GBA 557 Computer-based Data Communications	4 units 40 hours
GBA 560 Legal Environment of Information Systems	4 units 40 hours
GBA 577 Advanced IT Audit	4 units 40 hours
GBA 608/609 Managerial Accounting Issues	3/1* units 40 hours
GBA 615/616 Seminar in Organizational Behavior	3/1* units 40 hours
GBA 673/674 Management Information Systems Seminar	3/1* units 40 hours

Courses Not Included

GBA 565/566 Effective Presentations Using Technology	3/1* units 40 hours
GBA 691 Directed Study	4 units 40 hours
GBA 692 Independent Study	1 unit 10 hours
GBA 695 Business Research Project	4 units 40 hours

Hours for GBA 691, 692 and 695 can be applied to all areas or selected areas depending on the topic and subject matter the graduate student wishes to pursue.

*Note course is is 3 units lecture per 1 unit applied project or research paper. The university/ college did that for accreditation purposes to give its graduate core courses more distinction to applied business research. Same number of hours as a 4 unit but labeled 3/1.

Vrije University, Netherlands, Graduate IT/IS Audit Program Compliance Grid for the Model Curriculum

Figure 1—Audit Process Domain (Vrije U)				
Subtopic	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
IS Audit Function Knowledge	6	Laws and regulations: audit charter	**Auditing Basics**—Total 24 hours, of which about eight are on these subjects	8
		Nature of audit: demand for audits (e.g., agency theory, insurance hypothesis, information hypothesis)		
		Nature of IS audit: need for control and audit of computer-based IS		
		Types of audit and auditor: IS, external, internal, government/public sector		
		IS auditor responsibility, authority, and accountability: audit charter, outsourcing of IS audit activities		
		Regulation and control of IS auditing: ISACA standards, guidelines, Code of Professional Ethics; laws; regulations		
Fundamental Auditing Concepts	7	Materiality: application of materiality for IS audit compared to materiality for financial statement audit	**Auditing Basics**—Total 24 hours, of which about eight are on these subjects	8
		Evidence: types of evidence; meaning of sufficient, reliable, relevant evidence		
		Independence: need for independence in attitude and appearance, situations that may impair independence		
		Audit risk: inherent risk, control risk, detection risk		
		IS and general audit responsibilities for fraud		
		Assurance		
Standards and Guidelines for IS Auditing	5	Knowledge of ISACA Code of Professional Ethics	**Auditing Basics**—Total 24 hours, of which about eight are on these subjects (also treated in second- and third-year module and not counted here)	8
		Review of current ISACA IS Auditing Standards and Guidelines		
		Standards and guidelines specific to a region/country: ACM, AGA, AICPA, AITP, IFAC, IIA, ISO, NIA		
		IS audit practices and techniques		
Internal Controls Concepts Knowledge	13	Relevance, structure and indicators of effective IT governance for organizations and IS auditors; IT governance structure	**Basics for Managing Management Information—** Hours provided are an estimate of the total 84 hours of the module. Sarbanes-Oxley includes a three-hour **workshop** not counted here. Part of the 24 hours already registered for this subtopic.	24
		Internal control objectives; internal control and documentation of IS, COCO, COSO, King, Sarbanes-Oxley Act of 2002, SAS94		
		Control classifications: preventive, detective, compensating/corrective		0
		General controls: organizational, security, general operating and disaster recovery, development, documentation		

Figure 1—Audit Process Domain (Vrije U)				
Subtopic	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
		Application controls: control objectives; classifications of application controls, e.g., computerized/manual, input/processing/output, preventive/detective/corrective, audit trails		
		COBIT: Structure and relevance of COBIT for organizations and IS auditors		
Audit Planning Process	7	Strategic/tactical audit planning	**Basics for Managing Management Information—** Hours provided are an estimate of the total 84 hours of the module. This module treats eight cases for different types of business and government.	36
		Engagement letter: purpose and content of engagement letters		
		Risk assessment: risk-based auditing, risk assessment methods, standards: AS-NZ 4360, CRAMM		
		Preliminary evaluation of internal controls: information gathering and control evaluation techniques		
		Audit plan, program and scope: compliance vs. substantive testing, application of risk assessment to audit plan		
		Classification, scope of audits: e.g., financial, operational, general, application, OS, physical, logical		
Audit Management	5	Resource allocation/prioritization/planning/ execution/reassignments	**Basics for Managing Management Information—** Hours provided are an estimate of the total 84 hours of the module.	8
		Evaluating audit quality/peer reviews		
		Best practice identification		
		Computer information system (CIS) audit career development		
		Career path planning		
		Performance assessment		
		Performance counseling and feedback		
		Training (internal/external)		
		Professional development (certifications, professional involvement, etc.)		
Audit Evidence Process	12	Evidence: sufficient, reliable, relevant, useful	**Basics for Managing Management Information—** Hours provided are an estimate of eight of the total 84 hours of the module.	8
		Evidence gathering techniques, e.g., observation, inquiry, interview, testing		
		Compliance vs. substantive testing: nature of and difference between compliance and substantive testing, types of compliance test, types of substantive test		
		Sampling: sampling concepts, statistical and nonstatistical approaches, design and selection of samples, evaluation of sample results		
		Computer-assisted audit techniques (CAATs): need for, types of, planning for and using CAATs; continuous online auditing approach		
		Documentation: relationship with audit evidence; uses of documentation; minimum content; custody, retention, retrieval		

Figure 1—Audit Process Domain (Vrije U)				
Subtopic	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
		Analysis: judge the materiality of findings, identify reportable conditions, reach conclusions		
		Review: provide reasonable assurance that objectives have been achieved		
Audit Reporting Follow-up	3	Form and content of audit report: purpose, structure and content, style, intended recipient, type of opinion, consideration of subsequent events	**Basics for Managing Management Information—** Hours provided are an estimate of the total 84 hours of the module.	8
		Management actions to implement recommendations		
Total Hours	**58**		**Total**	**108**

Figure 2—Management, Planning and Organization of IS Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
IS/IT Management	10	IT project management	**Management of IT Organizations**—Hours provided are an estimate of the total 39 hours. **Audit of Business Processes in Very IT Dependent Organizations**—Total hours are 33 of which about eight are on this subject.	12
		Risk management: economic, social, cultural, technology risk management		
		Software quality control management		8
		Management of IT infrastructure and alternative IT architectures, configuration management		
		Management of IT delivery (operations) and support (maintenance)		
		Performance measurement and reporting: IT balanced scorecard		
		Outsourcing		
		Quality assurance		
		Sociotechnical and cultural approach to management		
IS/IT Strategic Planning	8	IS/IT strategic planning: competitive strategies and business intelligence, link to corporate strategy	**Management of IT Organizations**—Total 39 hours, of which about eight are on this subject **Audit of Business Processes in Very IT-dependent Organizations**—Total 33 hours, of which about eight are on this subject	8
		Strategic information systems frameworks and applications: types of IS, knowledge management, decision support systems; classification of information systems		8
		Management of IT human resources, employee policies, agreements, contracts		
		Segregation of duties		
		IS/IT training and education		
IS/IT Management Issues	9	Legal issues relating to the introduction of IT to the enterprise (international and country-specific)	**IT Legal Issues**—One module of 18 hours (this subject is part of most auditing modules)	18
		Intellectual property issues in cyberspace: trademarks, copyrights, patents		
		Ethical issues		
		Privacy		
		IT governance		
		IT/IS housekeeping		

Figure 2—Management, Planning and Organization of IS Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Support Tools and Frameworks	6	COBIT: *Management Guidelines*, a framework for IT/IS managers	Not done or already accounted for earlier in table	0
		COBIT: audit's use in support of the business cycle		
		International standards: ISOI7799, ITIL, privacy standards, COCO, COSO, Cadbury, King		
Techniques	4	Change control reviews	Part of **workshop** not counted here	0
		Operational reviews		
		ISO9000 reviews		
Total Hours	**37**		**Total**	**54**

Figure 3—Technical Infrastructure and Operational Practices Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Technical Infrastructure (Planning, Implementation and Operational Practices)	25	IT architecture/standards	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing—**is 186, of which about 52 hours are on these subjects.	52
		Hardware: all IT equipment, including mainframe, minicomputers, client-servers, routers, switches, communications, PCs, etc.		
		Software: operating systems, utility software, database systems, etc.		
		Network: communications equipment and services rendered to provide networks, network-related hardware, network-related software, use of service providers that provide communication services, etc.		
		Baseline controls		
		Security/testing and validation		
		Performance monitoring and evaluation tools		
		IT governance: maintaining it and making it work for IT		
		IT control monitoring and evaluation tools, such as access control systems monitoring or intrusion detection systems monitoring		
		Managing information resources and information infrastructure: enterprise management software		
		Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799		
		Issues and considerations of service center vs. proprietary technical infrastructures		
		Open systems		
Service Center Management: Maintain Information Systems and Technical Infrastruc-	12	Service center management and operations standards/guidelines: COBIT, ITIL, ISO17799	**Management of IT Organizations**—Total 39 hours, of which about 10 hours are on this subject **Audit of Business Processes in Very IT-dependent Organizations**—Total 33 hours, of which about eight are on this subject	10 8
		Change management/implementation of new and changed systems: organization of the tools used to control the introduction of new and changed products into the service center environment		
		Security management		

Figure 3—Technical Infrastructure and Operational Practices Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
tures Through Organiza-tions Dedicated to These Activities		Resource/configuration management: compliance with organization/IT operating standards, policies and procedures (i.e., proper use of computer languages)	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing**—is 186 hours, of which about 52 hours are on these subjects.	52
		Problem and incident management		
		Capacity planning and prognosis		
		Management of the distribution of automated systems		
		Administration of release and versions of automated systems		
		Management of suppliers		
		Customer liaison		
		Service level management		
		Contingency/backup and recovery management		
		Call center management		
		Management of operations of the infrastructure (central and distributed)		
		Network management		
		Risk management		
		Key management principles		
Total Hours	**37**		**Total**	**122**

Figure 4—Protection of Information Assets Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Information Assets Security Management	8	Information technology and security basics, concept for IT security, need of securing IT resources, policy framework on IT assets security, management of IT security, training	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing**— is 186 hours, of which about eight hours are on these subjects.	8
		Standards, compliance and assurance on IT security		
Logical IT Security	9	Components of logical IT security, logical access control issues and exposures, access control software	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing—**is 186 hours, of which about 40 hours are on these subjects.	40
		Logical security risks, controls and audit considerations (audit of logical access, security testing)		
		Logical security features, tools, procedures		
Applied IT Security: High-technology Resources	9	Communications and network security: principles of network security, client-server, Internet and web-based services, firewall security systems and other connectivity protection resources (e.g., cryptography, digital signatures, key management policies), intrusion detections systems, COBIT, system reviews	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing**—is 186 hours, of which about 24 hours are on these subjects.	24
		Mainframe security facilities		
		Basic database application and system security		
		Security in the system development and maintenance process		

Figure 4—Protection of Information Assets Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Physical and Environmental Security	3	Environmental issues and exposures: concepts on physical IT security	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing**—is 186 hours, of which about two hours are on these subjects.	2
		Physical access exposures and controls		
Total Hours	**29**		**Total**	**74**

Figure 5—Disaster Recovery and Business Continuity Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning	10	Management support and commitment to the process	The total of two modules—**Technique and Audit of Enterprise IT** and the **Audit of Midrange Computing—**is 186 hours, of which about eight hours are on these subjects. **Management of IT Organizations**—Total 39 hours, of which about four hours are on these topics **Audit of Business Processes in Very IT-dependent Organizations—**Total 33 hours, of which about four hours are on this subject	8
		Plan preparation and documentation		
		Management approval and distribution of the plan		
		Testing, maintenance and revision of the plan; training		4
		Audit's role		
		Backup provisions		
		Business continuity planning		
		Business impact analysis		4
Insurance	2	Description of insurance	Counted under **IT Legal Issues,** part of the 18 hours above.	0
		Items that can be insured		
		Types of insurance coverage		
		Valuation of assets: equipment, people, information process, technology		
Total Hours	**12**		**Total**	**16**

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
IS Planning	9	IS managing components (e.g., data processes, technologies, organization), understanding stakeholders and their requirements	**Applications in a Distributed Environment**—Total 78 hours, of which about 12 hours are for the third through fifth subjects mentioned here. ERP is mainly a case in the **workshop** for two groups (of the maximum of eight groups) and is not counted here.	12
		IS planning methods: system investigation, process integration/reengineering opportunities, risk evaluation, cost-benefit analysis, risk assessment, object-oriented systems analysis and design		
		ERP software enterprise applications integration		
Information Management and Usage	16	Monitoring service level performance against service level agreements, quality of service, availability, response time, security and controls, processing integrity, privacy, remedies, amending SLAs	**Management of IT Organizations**—Total 39 hours, of which about five hours are on these topics **Applications in a Distributed Environment**—Total 78 hours, of which about 20 hours are for the third through fifth subjects mentioned here	520
		Data and information: analyze, evaluate and design information architecture (i.e., the role of databases and database management systems, including knowledge management systems and data warehouses)		
		Data and application architecture (e.g., IS modeling, business models, processes and solutions); analysis, evaluation and design of an entity's business processes and business models		
		Information management (data administration, database functions and administration, DBA roles and responsibilities)		
		Database technology as tools for the auditor		
Development, Acquisition and Maintenance of Information Systems	12	Information systems project management: planning, organization, human resource deployment, project control, monitoring, execution	**Applications in a Distributed Environment**—Total 78 hours, of which about 20 hours are on the subjects are mentioned here	20
		Traditional methods for the system development life cycle (SDLC); analysis, evaluation and design of an entity's SDLC phases and tasks		
		Approaches for system development: software packages, prototyping, business process reengineering, computer aided software engineering (CASE) tools		
		System maintenance and change control procedures for system changes		
		Risk and control issues, analysis and evaluation of project characteristics and risks		

Figure 6—Business Application System Development, Acquisition, Implementation and Maintenance Area Topic Descriptions (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Impact of IT on the Business Processes and Solutions	4	Business process outsourcing (BPO) Applications of e-business issues and trends	**Applications in a Distributed Environment**—Total 78 hours, of which about eight hours are on the subjects mentioned here	8
Software Development	11	Separation of specification and implementation in programming Requirements specification methodology Algorithm design, sorting and searching algorithms File handling Linked lists and binary trees Database creation and manipulation Principles of good screen and report design Program language alignment	**Applications in a Distributed Environment**—Total 78 hours, of which about eight hours are on the subjects mentioned here	8
Total Hours	**52**		**Total**	**73**

Figure 7—Business Process Evaluation and Risk Management Domain (Vrije U)				
Subtopics	**Hrs**	**Description**	**Course(s) Covering Subtopic**	**Hours**
Audit and Development of Application Controls	19	Input/origination controls Processing control procedures Output controls Application system documentation Audit trails	**Audit of Business Processes in Very IT-dependent Organizations**—Total 33 hours, of which about five are on this subject **Applications in a Distributed Environment**—Total 78 hours, of which about 10 hours are on the subjects mentioned here	5 10
Total Hours	**19**		**Total**	**15**

Grand Total	**244**	**Total hours figures 1 through 7 Vrije University**	**Vrije University** Grand Total Workshop over a period of 18 weeks (maximum of six hours per week = 108 hrs) where each group carries out two cases Grand Total Post Graduate Course	 462 108 570

Supplemental Information

- The university's course objective is to teach a students enough to give them the basis to perform (and later manage) IT and IS audits.
- The post-graduate course attempts to include all the IS/IT audit education that is necessary. Undergraduate courses cannot be relied on to bring future auditors up to the graduate level. In other words, the Vrije University post-graduate course includes the required undergraduate information.
- The course lasts for two and one-half years and meets one day a week for six hours.
- The workshop is not accounted for within the profile because it is a learning-to-learn course with specific mentors per case. The first series of cases is: Audit of Quality Management Project, Audit of Key Management Procedures, Write an Audit Approach for a Conversion Process and Due Diligence Audit. The second series includes: SAP Audit of Operational SAP, Trusted Third-party Audit, Audit of Unicenter (now TNG) Pilot Project and Benchmarking for a Company. The students use an average of 45 class hours per person (excluding contact hours with the mentor) for the two audits together. The groups have a minimum of six students, which means each audit averages at least an assignment requiring approximately 135 hours. The workshop is 108 hours, of which 54 hours are contact hours (including the group presentations).
- Hours presented are contact hours.
- The grid is filled in at the subtopic level, which was not that difficult to do. Of course at this level of generality, the fit between the Vrije University modules and the profile is not perfect.

Appendix 5. Acronyms

ACM—Association for Computing Machinery
AGA—Association of Government Accountants
AICPA—American Institute of Certified Public Accountants
AITP—Association of Information Technology Professionals
COCO—Criteria of Control
COSO—Committee of Sponsoring Organizations of the Treadway Commission
IFAC—International Federation of Accountants
IIA—Institute of Internal Auditors
ISO—International Organization for Standardization
ITIL—Information Technology Infrastructure Library
NIA—National Institute of Accountants

Appendix 6. References

CISA Examination Areas, ISACA Certification Board, Rolling Meadows, IL, USA, 2003, *www.isaca.org/cisa*

COBIT (*Control Objectives for Information and related Technology*) 3rd Edition©, IT Governance Institute, Rolling Meadows, IL, USA, 2000, *www.isaca.org/cobit*

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

Lord, A. T.; "ISACA Model Curriculum 2004," *International Journal of Accounting Information Systems*, Volume 5, p. 251-265, 2 July 2004

Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Levels, 1st Edition, Information Systems Audit and Control Association, Rolling Meadows, IL, USA, March 1998