Development of an Interdisciplinary Information Technology Auditing Program

Chienting Lin, Li-Chiou Chen, *Pace University*

Abstract – This paper provided an example for the development of an interdisciplinary Information Technology (IT) Auditing curriculum by mapping the CNSSI /NSTISSI standards with the prevailing ISACA IT Auditing Model Curriculum. IT Auditing involves assisting public or private organizations in ensuring that their information technologies and business systems are adequately protected and controlled. Consequently, IT Auditing professionals need to have a solid grounding in information technology, information assurance, auditing process, as well as regulatory and compliance frameworks. Through our standard mapping processes, we were able to discover the discrepancies between IA and Auditing and proceeded to redesign our current IA curriculum. Specifically, we have proposed a new IT Auditing course that addresses IT Auditing-specific topics, as part of an IT Auditing concentration in both undergraduate and graduate levels. Our results will help shed light on how other CAEIAE institutions can enhance their current IA curriculum by collaborating with other disciplines to help prepare their students for emergent IA careers in business or healthcare.

Index terms – IT Auditing, Regulatory Compliance, Information Assurance Curriculum

I. Introduction

Internal controls and auditing has been an important issue in corporate governance. In order to tighten internal control process, Sarbanes-Oxley Act (SOX) was enacted in the midst of various financial frauds including Enron and WorldCom [1]. To be compliant with such government regulations, organizations are in need of professionals who can perform Information Technology (IT) Auditing. IT Auditing professionals are required to have substantial knowledge in both auditing process and information technology in order to protect corporate information assets.

IT Auditing is an interdisciplinary area that requires expertise across Information Assurance (IA) and Accounting. Although typically IA curriculum overlaps with the knowledge background needed for training IT Auditing professionals, it still cannot cover the entire IT Auditing area. The purpose of the paper is to provide an example for the development of an interdisciplinary IT Auditing curriculum by mapping the prevailing CNSSI[1]/NSTISSI[2] standards with the Information Systems Auditing and Control Association (ISACA[3]) IT Auditing Model Curriculum, as recommended by IT Auditing industry practitioners. Since CNSSI/NSTISSI standards have been mapped extensively to IA curriculum offered by the universities designated as NSA's Centers of Academic Excellence in Information Assurance Education (CAEIAE)[4], our mapping can provide CAEIAE universities with suggestions on how to enhance their current IA curriculum in order to train IT Auditing professionals.

The organization of the paper is as follows: Section II will provide background for IT Auditing and CNSSI/NSTISSI standards, as well as the motivation for the mapping process. Section III will provide the mapping between IT Auditing topics and CNSSI/NSTISSI standards. Section IV will discuss the discrepancies between IT Auditing topics and knowledge areas in CNSSI/NSTISSI standards. Section V will present a proposed IT Auditing course to enhance the existing IA curriculum. Conclusions and suggestions for future work are followed.

II. Background

IT Auditing involves understanding the auditing process in order to provide technology audit services in accordance with audit standards, guidelines, and best practices. IT Auditing process is designed to assist the organization in ensuring that its information technology and business systems are adequately protected and controlled. Thus, IT Auditing requires interdisciplinary

Both Chienting Lin (clin@pace.edu) and Li-Chiou Chen (lchen@pace.edu) are assistant professors in Seidenberg School of Computer Science and Information Systems, Pace University, New York.

[1] Committee on National Security Systems Instruction.
[2] National Security Telecommunications and Information Systems Security Instruction.
[3] ISACA stands for Information Systems Audit & Control Association. It is an international organization of IT-related professionals, including IS auditor, consultant, educator, IS security professional, regulator, chief information officer and internal auditor.
[4] See NSA's National Centers of Academic Excellence, available at http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

ISBN 1-933510-96-7/$15.00

domain of knowledge across information technology, information security and controls, systems development, and auditing.

We are interested in developing IT Auditing curriculum through enhancing our current IA curriculum. Our interests are partly motivated by the imbalance of supply and demand of qualified IT Auditing professionals. On the demand side, we have recently witnessed a strong job growth in IT Auditing. Corporations are now required to be in compliance with various government regulations on internal controls and information security/privacy, including the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA), etc. The demand has helped to create highly sought-after certifications such as the Certified Information Systems Auditor (CISA), offered by ISACA. The CISA exam is designed to certify audit skills, both technical and ethical. The median salary[5] for CISA holders is around $77,311 per year. On the supply side, IT Auditing is a new niche area for current computing programs which could reinvent themselves to supply computing professionals with interdisciplinary background in auditing. The enrollment of the undergraduate computing programs in the US has dropped significantly in the recent years. According to the Computer Research Association[6], the enrollment in Computer Science (CS) has declined since its peak in 2000 and had dropped 18 percent between 2005/2006 and 2006/2007. There are many reasons that contribute to the declining enrollment of computing undergraduates. One of them is the gap between the knowledge scope of our current computing curricula and the expectations of the IT industry. One way to bridge the gap is to provide students with the required knowledge in specific computing applications in additional to general computing principles and theories. IT Auditing is one of these areas that will allow students to broaden their knowledge scope by acquiring a solid background in both computing theories and information assurance, in particular, IT Auditing.

III. Integrating Information Technology Auditing Into Information Assurance Curriculum

ISACA IT Auditing Model Curriculum [2], published and advocated by ISACA, includes seven topic areas as shown as in Table 1. These topics range from business process management, information security, to auditing processes. The ISACA model curriculum was developed to provide universities with a basic framework for organizing the common body of knowledge in IT Auditing in order to effectively cultivate IT auditors at both undergraduate and graduate levels.

All CAEIAE universities have to be certified for NSTISSI 4011 and at least one of the other CNSSI/NSTISSI standards. Based on Presidential Decision Directive 63 on Critical Infrastructure Protection [3], the National Security Telecommunications and Information Security Systems Commission (NSTISSC), later known as the Committee on National Security Systems (CNSS), had developed the CNSSI/NSTISSI standards for training information systems security professionals in order to secure federal government systems: NSTISSI 4011 is the general standard for information systems security professionals; CNSSI 4012 is for senior system managers; CNSSI 4013 is for system administrators in information systems security; CNSSI 4014 is for information systems security officers; NSTISSI 4015 is for system certifiers and CNSSI 4016 is for risk analysts.

IA academic programs have faced several challenges recently. As a way to broaden the appeal of their graduates as well as expanding the scope of their computing programs, many computing programs have either integrated IA curriculum into existing Information Technology, Information Systems or Computer Science programs [4-8], or at least designed a single course to cover IA topics [9]. However, educators have proposed changes in IA curriculum to cover both technical and non-technical aspects of information security in order to keep up with the fast-changing security requirements for the public, the industry, and the government [8]. In addition, surveys have found that the CNSSI/NSTISSI standards may not be appropriate for college-level computer security programs, since they were originally developed as government training standards [10].

Our goal is to enhance our IA curriculum by integrating IT Auditing topics such that our IA curriculum is not only mapped to government training standards but also covers industry standards and needs. We mapped the ISACA IT Auditing Model Curriculum topics with the knowledge areas in CNSSI/NSTISSI standards, as shown in Table 1. Since our current curriculum is already certified for NSTISSI 4011 and CNSSI 4013, we were able to discover knowledge areas that are not in our current IA courses but are required for IT Auditing through the mapping results. In particular, we have discovered six topic areas in IT Auditing that are not covered by CNSSI/NSTISSI standards, referred as N/A in Table 1. These areas include standards and guidelines for IS Auditing, internal controls concepts knowledge, audit reporting follow-up, insurance, and impact of IT on the business processes and solutions.

[5] The median ITA salary is estimated by PayScale.com as of February, 2009.
[6] http://www.cra.org/

ISBN 1-933510-96-7/$15.00

ISACA IT Auditing Model Curriculum Topics	**CNSSI/NSTISSI Standards Mapping**
1. Audit Process Domain	
Information Systems (IS) Audit Function Knowledge	4011 – Auditing and Monitoring
Fundamental Auditing Concepts	4013 – Audit Tools 4014 – Monitoring and Auditing Policy
Standards and Guidelines for IS Auditing	N/A
Internal Controls Concepts Knowledge	N/A
Audit Planning Process	4013 – Administrative Countermeasures: Audit
Audit Management	4015 – Performing Certification Analysis: Audits
Audit Evidence Process	4012 – Audit Trail Policy, Auditable Events
Audit Reporting Follow-up	N/A
2. Management, Planning and Organization of IS Domain	
IS/IT Management Strategic Planning	4011 – Risk Management, System Life Cycle Management 4012 – Risk Management, Life Cycle Management
IS/IT Management Issues	N/A
Support Tools and Frameworks	4012 – Federal Information Security Management Act (FISMA)
Techniques	4016 – Certification and Accreditation
3. Technical Infrastructure & Operational Practices Domain	
Technical Infrastructure (Planning, Implementation And Operational Practices)	4011 – Automated Information Systems (AIS) Basics: Hardware, Software, Firmware; System Operating Environment: Telecommunications 4013 – Network & Operating System
Service Center Management: Maintain Information Systems and Technical Infrastructures Through Organizations	4014 – Risk and Configuration Management 4016 – Life Cycle Duties
4. Protection of Information Assets Domain	
Information Assets Security Management	4011 – Information Security 4016 – Countermeasures
Logical IT Security	4012 –Access Controls 4015 – Access Controls Policies
Applied IT Security: High-technology Resources	4011 – Network Security& Transmission Security 4012 – PKI
Physical and Environmental Security	4011 –Physical Security Measures
5. Disaster Recovery and Business Continuity Domain	
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning	4011 – Contingency Planning/Disaster Recovery 4015 – Contingency Planning
Insurance	N/A
6. Business Application System Development, Acquisition, Implementation and Maintenance Domain	
IS Planning	4011 – Concepts of Risk Management
Information Management and Usage	4012 – Storage & System Architecture 4013 – Risk Management
Development, Acquisition And Maintenance of Information Systems	4011 Systems Life Cycle Management
Impact of IT on the Business Processes and Solutions	N/A
Software Development	4016 – Life Cycle Duties
7. Business Process Evaluation and Risk Management Domain	
Audit and Development Of Application Controls	4011 Auditing and Monitoring; 4015 Audits

Table 1: Mapping between ISACA Model Curriculum Topics and CNSSI/NSTISSI standards

IV. Topic Differences Between IT Auditing and CNNSI/NSTISSI

During the course of the mapping, we have noticed that there are indeed differences in applications and gaps in coverage while many topics are complimentary. ISACA guidelines are geared more toward business organizations and applications, while the CNNSI/NSTISSI standards emphasize applications in government and military

ISBN 1-933510-96-7/$15.00

applications. When compared to CNNSI/NSTISSI standards, the IT Auditing model curriculum exhibits the following major differences:

1) Emphasis on enterprise risk management issues: This emphasis leads to implementation of various security policies and resultant internal controls, e.g., controls that are preventive, detective, or corrective in nature, with an aim for fraud detection. It Auditing also differs from CNNSI/NSTISSI standards by mandating the inclusion of proper risk transfer strategies such as acquiring cyber security insurance.

2) Coverage of industry-specific regulatory and compliance frameworks: On one hand, business applications need to address industry-specific regulations such as HIPAA, SOX, and GLBA, etc. Consequently, regulation compliance requires organizations to adopt various governance frameworks such as the Committee of Sponsoring Organizations (COSO) and the Control Objectives for Information and related Technology (COBIT). On the other hand, CNNSI/NSTISSI standards mostly address regulatory requirements for information systems within or supporting federal government such as the Federal Information Security Management Act (FISMA).

3) Adherence to audit standards or processes: ISACA IS auditing standards [11] offer a comprehensive treatment of auditing information systems which contains IT components. These standards provide guidelines about how to set up an audit charter, how to ascertain audit materiality, how to gather audit evidence through various sampling techniques, as well as how to handle audit evidence. Additionally, the Information Technology Assurance Framework (ITAF) [12] also provides a model that guides the design and reporting of IT audits. In comparison, auditing topics in CNNSI/NSTISSI standards mostly focus on "auditable events," such as reviewing system or network logs, which are more operational in nature.

V. Proposed IT Auditing Curriculum

To address the aforementioned gaps in the coverage of topics, we proposed an IT auditing course which can be integrated into existing IA curriculum to broaden its appeal to traditional Accounting/Auditing majors. The proposed course will enable business majors to benefit from a comprehensive treatment of IT Auditing and IA topics while allowing security majors to learn about how to apply IA principles in a business setting. The proposed course topics are listed in Table 2.

We have surveyed currently available IT Auditing textbooks and found suitable text such as [13]. We also plan to adopt ISACA's CISA Review Manual and test banks [14]. For hands-on laboratory exercises in this course, we plan to utilize Computer-Aided Auditing Technique (CAAT) tools such as the ACL (Auditing Command Language) software.

Course Topics	Subtopics
IT Auditing Frameworks	• Standards and Guidelines for IT Auditing, Internal Controls & Audit Planning • Audit Evidence Process & Audit Reporting • Control Framework: COBIT, COSO, ISO 27001-2
IT Lifecycle Management & Service Delivery	• Infrastructure Planning & Implementation • Service Level & Service Center Management • System Resiliency Tools and Techniques

Table 2. Topics in the proposed IT Auditing course

A single IT Auditing course would be insufficient to fully address the wide range of topics required by IT Auditing. Therefore, we proposed an interdisciplinary IT Auditing curriculum that combines existing IS/IT courses with traditional IA specific courses. As shown in Table 3, the new curriculum is designed based on the common body of knowledge in the ISACA IT auditing Model Curriculum and the CISA job areas.

IT Auditing Curriculum Topics	Corresponding Course
IT Auditing Process	IT Auditing
IT Governance	IT Auditing, Accounting Information Systems
Systems & Infrastructure Lifecycle Management	Systems Analysis & Design
IT Delivery & Support	Systems Analysis & Design
Protection of Information Assets	Overview of Information Security, Network/Web Security, Computer Forensics
Business Continuity & Disaster Recovery	Overview of Information Security, IT Auditing

Table 3. IA & IS courses mapped to IT Auditing topics

ISBN 1-933510-96-7/$15.00

This interdisciplinary curriculum will include two business oriented courses – Accounting Information Systems and Systems Analysis and Design from the Accounting and IS departments, one new course - IT Auditing, and three existing IA courses including: Overview of Information Security, Network/Web security and Computer Forensics. The target audience for this newly proposed IT Auditing curriculum will include our undergraduate majors in Accounting, Information Systems/Technologies, and MBA-IS and MS-Accounting students. Graduate-level version of the courses will include additional requirements for research papers and more comprehensive project requirements.

VI. Evaluations

Although the proposed IT Auditing curriculum has not been offered at this point, we have developed an assessment plan for future implementation. The plan aims at assessing the proposed curriculum from both the programmatic objectives and the course specific learning outcomes.

Our programmatic objective is to bring faculty and students across different academic disciplines to jointly cultivate expertise in IT Auditing, while enhancing the marketability of our IS/IT students. Consequently, our assessment will focus on both the interdisciplinary nature of the curriculum, as well as the effectiveness of our proposed contents. Specifically, our assessment plan will collect the following quantitative measures: 1) Student exam results: We will incorporate selective questions from the official CISA Review Manual from ISACA to gauge student learning results; 2) Student placement: We hope to track the number of students who obtain IT Auditing jobs after going through the proposed curriculum. To assess the specific learning outcomes from the new IT auditing course, we will collect data on course content, student project reports, and student satisfaction. These data will be evaluated both internally as well as externally by getting feedback from local ISACA members and/or other IT Auditing practitioners.

VII. Conclusions

In order to address the interdisciplinary need for training IA professionals in many emergent applications, it is time for IA programs to collaborate with business or healthcare departments to jointly create new and innovative educational programs. We provided one such example by combing IA courses with auditing principles offered by the Accounting departments in business schools, in order to effectively address the burgeoning need for qualified IT Auditing professionals.

In this paper, we examined the topic differences between the ISACA IT Auditing Model Curriculum and the CNNSI/NSTISSI standards. We also proposed a new IT auditing course to cover the topics not currently covered by the CNNSI/NSTISSI standards but are essential for IT Auditing professionals. Our examination of the gaps between the two areas will be helpful for CAEIAE universities when they are in the process of designing new interdisciplinary IA programs such as IT Auditing.

We will further implement course materials for the new IT Auditing course and assess the outcomes of our IT auditing curriculum using various quantitative and qualitative measures. We are also in the process of looking into other similar opportunities such as HIPAA compliance for nursing/healthcare programs, as well as Web Security for E-Commerce/Marketing programs. We believe that the opportunities for applying IA principles in other emergent areas are plenty and hope we have helped shed some light on how such efforts can be accomplished.

VIII. References

[1] K. F. Brickey, “From Enron to WorldCom and Beyond: Life and Crime After Sarbanes-Oxley,” *Washington University Law Quarterly*, vol. 81, June 1st 2003.

[2] ISACA, “ISACA Model Curriculum for IS audit and Control,” 2004, available at www.isaca.org.

[3] White House, “PDD 63, Critical Infrastructure Protection,” 1998.

[4] T. Bacon and R. Tikekar, “Experiences with developing a computer security information assurance curriculum,” *Journal of Computing Sciences in Colleges*, vol. 18, pp. 254 - 267 April 2003.

[5] M. J. Dark, J. J. Ekstrom, and B. M. Lunt, “Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice,” *Journal of Information Technology Education*, vol. 5, pp. 389-403, 2006.

[6] S. J. Geoghegan, “The Development of an Information Assurance Program,” *Journal of Computing Sciences in Colleges*, vol. 23, pp. 116-123, 2008.

[7] A. J. A. Wang, “A security thread in a thread-based curriculum,” in *Conference On Information Technology Education*, Cincinnati, OH, 2008, pp. 193-200.

[8] M. Hentea, H. S. Dhillon, and M. Dhillon, “Towards Changes in Information Security Education,” *Journal of Information Technology Education*, vol. 5, pp. 221-233, 2006.

ISBN 1-933510-96-7/$15.00

[9] K. Jiang and M. Bannister, "Secure Information at Your Fingertips" -- Just One Course can Help," in *The 12th Colloquium for Information Systems Security Education*, Dallas, TX, 2008.

[10] C. Taylor, J. Alves-Foss, and V. Freeman, "An Academic Perspective on the CNSS Standards: A Survey," in *The 10th Colloquium for Information Systems Security Education*, Adelphi, MD, 2006.

[11] ISACA, "ISACA Auditing Standard," 2004, available at www.isaca.org.

[12] ISACA, "Information Technology Assurance Framework," 2004, available at www.isaca.org.

[13] S. Senft and F. Gallegos, *Information Technology Control and Audit*, 3rd Ed. Boca Raton, FL: Auerbach Publications, 2009.

[14] ISACA, *CISA (Certified Information Systems Auditor) Review Manual 2009*. Rolling Meadows, IL: Information Systems Audit and Control Association (ISACA) Press, 2008.

ISBN 1-933510-96-7/$15.00