Education in IT controls at the Faculty of Computer and Information Science in Ljubljana

Viljan Mahnic[1] and Natasa Zabkar[2]

[1] University of Ljubljana, Faculty of Computer and Information Science
Trzaska 25, SI-1000 Ljubljana, Slovenia
[2] Triglav Insurance Company Ltd Miklosiceva 19, SI-1000 Ljubljana, Slovenia

1 Introduction

The importance of information technology (IT) controls is increasing, thanks to the security demands of e-commerce. The IT security is just one of the three business requirements for information, as defined by COBIT. The other two requirements are quality requirements and fiduciary requirements [5, pg. 13]. Nevertheless, IT security is often regarded by IT professionals as the most important requirement. White-collar crime, information theft, computer fraud, information abuse and other IT control concerns are getting high visibility with the extensive use of e-commerce [7, pg. B]. A possible reason for this might be that abuses of e-commerce solutions have been largely publicized, while information about internal IT abuses often exist only in dark figures. It has been very common to expect from IT professionals to develop IT solutions that satisfy security requirements.

IT controls are closely related to IS auditing. While managers are responsible for IT controls (”to ensure”), it is auditors’ responsibility to evaluate these controls according to the requirements mentioned earlier (”to assure”). At present, it is mainly IT auditors community that is concerned about IT controls. Even though they can use proactive approach, the majority of their work is still of reactive nature. After the design phase, it costs four times more to retrofit controls into a system, after programming eight times more and after implementation 16 times [8, pg. 45]. Using proactive approach IT professionals could avoid the retrofitting costs. IT control/audit education can be regarded as a preventive measure. Knowledgeable and well educated IS control/audit professionals are needed to ensure and assure the security of IS [7, pg. B].

One third of all US companies employ IS auditors [8, pg. 44]. In Slovenia, almost 33% of surveyed companies [12, pg. 14] did not have IS audit and did not plan to have any. In the majority of the companies (42%) IS audit has been performed by the accounting auditors, and only 5% have already experienced an IS audit performed by the IS auditors.

In the USA, companies have been unable to hire enough IS auditors, since starting salaries for audit jobs are lower than for jobs in technology, and majority of students rather start as a programmer or database analyst than as an auditor [13, pg. 13]. That is why companies have started to outsource the IS audit function. In Slovenia, majority of companies (55%) is not well informed about IS audit [12, pg. 14], so the demand for IS auditors is not very high. But, recent changes in legislation indicate that IS audit is becoming more important for banks, financial institutions, insurance companies, public services institutions, enterprises with shares quoted on the stock exchange and for brokerage houses [17]. It is very likely that IT professionals will have to participate in IS audits either as auditees or auditors. The knowledge on IT control/audit will become a competitive advantage. Universities offering courses in IS control/audit will differentiate in the market by providing employers with IT professionals who already possess IS control/audit knowledge.

The aim of this paper is to recommend a solution that would make the Faculty of Computer and Information Science in Ljubljana more competitive in the e-commerce world. Therefore, we shall explore the possibilities of expanding its (post)graduate curriculum.

2 IS control/audit education

According to [7], there are three sources of obtaining formal IS auditing education: (1) mixture of on-the-job training and in-house programs; (2) workshops/seminars presented by professional organizations or vendors and (3) traditional university academic environment. Even 70% of training is on-the-job and only 8% learned in school [7, pg. 4]. This shows the niche that universities could take the advantage of and provide the necessary curriculum.

At present, IS auditors are usually holders of at least two different titles: (1) college/university degree (various undergraduate majors, different types of masters' degrees) and (2) professional certification (CXX type certification like CISA (certified information systems auditor), CPA (certified public accountant), CIA (certified internal auditor) etc). While college degree is required by employers, professional certification is considered to be a plus, not a requirement [2, pg. 36]. According to [14, pg. 41] master's degree (esp. MBA (master of business administration)) and professional certification (esp. CISA and CPA) provide IS auditors with long-term benefits and/or with promotions.

Information Systems Auditing and Control Association (ISACA) offers CISA certification, which has been recognized as the international standard of achievement among IS audit, governance, control and assurance professionals [2, pg. 35]. The purpose of CISA is to evaluate candidates' understanding of auditing and systems concepts and their application, the skills that enable candidates to perform better on their undergraduate and (post)graduate examinations [3, pg. V]. CISA holders have to pass CISA examination and keep up to date by fulfilling continuing education (CE) requirements [2, pg. 35]. Exams for professional certification can be taken in the last undergraduate quarter or semester. These certifications help undergraduates to look on their college program as an integrated program which prepares them for professional practice rather than a number of individual courses required for graduation [3, pg. 11].

In Slovenia, IS auditors mainly educate themselves through on-the-job training and through workshops and seminars organized as continuing professional education programs by the Slovenian Institute of Auditors. In order to receive a license to practice in Slovenia one must fulfill the following conditions: (1) Bachelor's degree; (2) CISA exam (prepared and graded by the ISACA); (3) ”Auditing and International Auditing Standards” exam (prepared, administered and graded by the Slovenian Institute of Auditors) and (4) ”Legislation of Information Systems in the Republic of Slovenia” exam (prepared, administered and graded by the Slovenian Institute of Auditors). At present, there are 18 IS auditors registered by the Slovenian Institute of Auditors [17]. The control/audit education in the university academic environment could be beneficial for increasing this number.

College curriculum is often prepared so that it covers professional certification areas (e.g. accounting curriculum and CPA). In 1997, more than 20 colleges and universities in the US had internal auditing program [10, pg. 51]. But, it has been noted, that computer science and IS programs often spend too much time on technical engineering issues, while information problems of management and accounting are not being covered. The Association of Information Technology Professionals proposed an elective course on IS auditing in their Model Curriculum for undergraduate computer IS education in 1981 [7, pg. 5]. According to [18] there are seven colleges and universities in the USA offering degrees in IT control.

The University must be independent and objective. Therefore more than one standard should be taught in the IS control/audit educational process. ISACA has developed a standard that is open system and is well recognized internationally: Control Objectives for Information Technology (COBIT). Its primary reference material includes more than 30 standards, such as BS7799 - Information Security Management (British Standards Institute, London, 1999); ISO IEC JTC1/SC27 Inf. Technology - Security: International Organization for Standardization (ISO) Technical Committee on Information Technology Security, Switzerland, 1998; Common Criteria and Methodology for IT Security Evaluation; CSE (Canada); SCSSI (France); BSI (Germany); NLNCSA (Netherlands) etc.). In this paper we shall limit ourselves to COBIT, even though other standards could be used as well (an example of IS audit using standards NIVRA and COBIT can be found in [9]).

The 1996 COBIT and the 1996 CISA domains were the basis for developing ISACA Model Curricula. This curricula have been developed by the global committee [7, pg. B] from 14 countries, representing faculty from 15 undergraduate and graduate schools and staff from 20 companies. The purpose of this model is to propose IS auditing curricula at the undergraduate and (post)graduate levels and to provide a better theoretical and empirical knowledge base for IS control/audit function.

For undergraduate studies, ISACA Model Curricula proposes courses classified into three groups: (1) accounting; (2) information systems and (3) internal auditing. Some examples of IS audit education at the undergraduate level include: Bentley College (US), Bowling Green State University (US), Curtin University of Technology (AUST) and others. The example of Californian State Polytechnic University, Pomona (Spring 1997 Syllabus) is very convenient to use as an example [7, pg. 26]. Accounting and internal auditing are traditionally taught at the business schools, while information systems are taught at the computer science schools. The best program could be achieved through interdisciplinary program that would include professors from the both faculties. However, this type of changes are more common at the (post)graduate level.

For (post)graduate studies, ISACA Model Curricula proposes courses classified into four sections [7, pg. 11]:

- basic understanding (IS Management, Auditing Practice and Theory, International Business/Business Organization/Finance);

- required IS auditing related courses (Legal Environment of IS, IS Auditing/CAATs, Security and Privacy in IS, Advanced Networks and Communication Issues, Advanced IS Auditing);
- directed electives (courses relating to students' research projects or thesis, offered by other Universities or departments or off-campus distance learning);
- business research methods and project thesis (the aim of this section is to provide training, direction and guidance in research/sampling tools, techniques and methodologies).

ISACA recommends Academic Relations Committees in their chapters to work closely with the academic community. ISACA members could take part in teaching some of the courses by providing students ”real world” experience [4]. It is recommended to have University Advocate (the liaison at the University for ISACA chapter) who would coordinate these activities.

In the next section we shall see how the ISACA (post)graduate model could be used for extending (post)graduate curriculum at the Faculty of Computer and Information Science in Ljubljana.

3 The Faculty of Computer and Information Science

The study programs of the Faculty of Computer and Information Science in Ljubljana are registered with the European Federation of National Engineering Associations (FEANI) and meet the criteria for the title EUR ING [15].

The Faculty offers two undergraduate educational programs: (1) a four year program (abbreviation 4UG) for the degree of Dip. Ing. of Computer and Information Science and (2) a five year ”university” program (abbreviation 5UG) for the degree of University Dipl. Ing. of Computer and Information Science. Both programs have three elective modules: (1) information science; (2) computer logic and systems and (3) computer software. A four year program is more application oriented, while the five year program is more theoretical and is mandatory for the postgraduate studies.

Postgraduate programs consist of two years of course work, followed by a Masters thesis (M. Sc. degree) and subsequently by a Doctoral thesis (Ph. D. degree). There are two postgraduate programs: (1) computer and information science (abbreviation CPG) and (2) information systems and decision making (abbreviation IPG).

COBIT has been already taught in the following two courses: (1) ”Technology of information systems” (5UG), where it is presented next to the quality standards such as ISO 9000, CMM and SPICE and (2) ”E-commerce” (PG), where it is presented next to the standards such as ISO and BS 7799. IS audit/control is considered in the following three courses: (1) ”Design and Management of Information Systems” [5UG]; (2) ”Accounting” [4UG] and (3) ”Project management and Organization of Information Systems” [4UG]. These courses cover only part of CISA and COBIT domains.

Since undergraduate program is more difficult to change from the administrative point of view, we have decided to focus our efforts on the (post)graduate program. There is one (post)graduate course (”E-commerce”) where some of CISA and COBIT domains are taught. This could not fulfill our requirements. Therefore, we introduced a new set of IS control/audit (post)graduate courses that would cover all CISA and COBIT domains.

The ISACA model assumes there is a special (post)graduate program dedicated to IS control/audit. This solution might be considered as a long term solution, if the demand for IT security professionals continues to increase. The model curricula is a guideline and not an absolute criteria, so we have adjusted the ISACA model to the requirements of the Faculty of Computer and Information Science in Ljubljana.

We have selected some courses from the first and the second section of the ISACA (post)graduate model and included one case study in each course. The criteria for selection was to fulfill all three COBIT business requirements (security, quality, fiduciary requirement). But, since basics need to be taught first, we have selected ”Information Systems Auditing” (”IS Audit: Introduction”) from the first section. From the second section we have selected ”Legal Environment in Information Systems” (”IS Audit: Fiduciary Requirements”) and ”Security and Privacy in Information Systems” (”IS Audit: Security Requirements”). Then we introduced a new course that deals with auditing the IS management and the IS development: ”IS Audit: Quality Requirements”.

We have compared our choice to the curriculum of seven US universities and colleges [18] and found out that our approach was similar to the solution in California State Polytechnic University which offers six (post)graduate classes: (1) ”Advanced IS Auditing”; (2) ”Management IS”; (3) ”Legal Environment of IS”; (4) ”Security and Privacy of IS”; (5) ”System Design and Analysis” and (6) ”Cyberspace as a business tool”. The course ”System Design and Analysis” is especially important, since it matches the quality requirements.

Our proposition is just one possible solution and is meant to be a starting point. For a better view of this solution some specifics are presented further on.

4 Proposition

The proposed structure of the four IS control/audit courses is given in the form of tables. In one column there is a general description and in the other specifics can be found. After that, a short description is given.

The auditing phase could be presented using ISACA COBIT Generic Audit Guideline [5], with the following four steps: (1) obtaining an understanding; (2) evaluating the controls; (3) assessing compliance and (4) substantiating the risk. For other phases one of the possible solutions is presented in [11], where the audit steps are: (1) agree the details with the auditee; (2) set down the facts; (3) identify risks and controls; (4) test identified controls; (5) report what is missing or not applied; (6) discuss solutions and obtain responses and (7) complete the draft report. Also Follow-up and Control Self-Assessment should be introduced.

According to [5] security requirements have three key elements: (1) confidentiality; (2) integrity and (3) availability. Firstly standard BS 7799 would be introduced, followed by ISACA Control Objectives for NetCentric Technology, which covers Intranet/Extranet/Internet, Online Transaction Processing and Data Warehouse. This standard represents a specific application of ISACA’s COBIT [6].

Table 1 IS Audit: Introduction

Nr	General	Specifics
1	Definition and Standards	Auditing standards ISACF General Standards for IS Auditing ISACF Statements on IS Auditing ISACA Audit Guidelines COBIT, CIPFA, NIVRA etc.
2	Pre-auditing phase	Risk analysis Inherent risk, Control risk, Detection risk Risk assessment techniques
3	Auditing phase	Interviews, questionnaires, control flowcharts Performance monitoring tools Sampling Compliance testing, substantive testing Computer assisted auditing techniques
4	Post-auditing phase	Reports Follow up Control Self-Assessment
5	Case study	

According to [5] quality requirements have three key elements: (1) quality; (2) cost and (3) delivery. Firstly, some quality standards would be introduced, like ISO 9000-3, SPICE and CMM. After that, ISACA Control Objectives could be used. COBIT provides a foundation for control model over information technology in support of business processes. COBIT is a set of 34 Control Objectives, one for each IT Process, that are grouped into four domains [5]: (1) planning and organization (strategy and tactics, compliance of the information architecture and business strategy, organizational and technological infrastructure); (2) acquisition and implementation (identification, development, acquisition, implementation and maintenance of IT solutions); (3) delivery and support (service level, security, continuity, training, application controls) and (4) monitoring (assessment of the quality of IT processes and their compliance with control requirements). All four domains would be presented from the quality point of view.

According to [5] fiduciary requirements have three key elements: (1) effectiveness and efficiency of operations; (2) reliability of information and (3) compliance with laws and regulations. These have been defined in the COSO (Committee of Sponsoring Organizations of the Treadway Commission-Internal Control) Report. Reliability of information is expanded to include all information, not just financial.

IS audit should be presented like fun or adventure, so that students would feel like they too could become detectives and heroes for their agency or firm [1, pg. 41]. This can be reached by using the case studies and examples from ”real world”, provided through coordination with the local ISACA Academic Relations Committee.

5 Conclusion

The importance of e-commerce is proportional to the importance of e-commerce security. The number of IT professionals who want to be proficient in IT controls, especially IT

Table 2 IS Audit: Security Requirements

Nr	General	Specifics
1	Definition and Standards	Confidentiality, Integrity, Availability COBIT, BS 7799, Orange book
2	Access Controls	Logical access Physical access Environmental access Data access
3	Net Centric Controls	Security design Electronic cash, internet payment Encryption ISACA Control Objectives for Net Centric Technology
4	Disaster Recovery Planning	Business Continuity Plan
5	Case study	

Table 3 IS Audit: Quality Requirements

Nr	General	Specifics
1	Definition and Standards	Quality, Cost , Delivery COBIT, ISO 9000-3, SPICE, CMM etc.
2	IT Governance	COBIT: Planning and Organization, Monitoring
3	IS Development	Process quality COBIT: Acquisition and Implementation COBIT: Delivery and Support Input controls Processing controls Output controls
4	IT Quality	Product quality Customer satisfaction
5	Case study	

security, is increasing. So far, IT control/audit has been taught at the Faculty of Computer and Information Science in Ljubljana in few different subject at the (post)graduate level.

In this paper we propose systematic approach to (post)graduate IT control/audit education at the Faculty of Computer and Information Science in Ljubljana by introducing four new courses. The structure of these courses is based on the ISACA model curricula and combined with current COBIT and CISA domains. One subject is dedicated to control/audit basic concepts. Each of the other three courses satisfies one of the COBIT business requirements: (1) security; (2) quality and (3) fiduciary requirements.

This approach is just one of possible solutions. We hope that implementation of this proposal will help (post)graduate students to improve the security level of e-commerce.

References

[1] Buxton, Brian M.: ”Information Systems Auditing In Developing Economies - The Bosnian Challenge”. ISACA: IS Control Journal, Volume 6, 2000. pp. 39-43.

Table 4 IS Audit: Fiduciary Requirements

Nr	General	Specifics
1	Definition and Standards	Definition Segregation of duties and responsibilities
2	Law Regulations	Legislation regarding privacy Legislation regarding intellectual property Electronic Commerce and Electronic Signature Other Acts
3	Accounting Standards	Internal auditing, internal control COSO report
4	Computer Crime	Types of computer crime Computer Ethics Viruses, Hackers and other attacks Evidence
5	Case study	

[2] Dito Arnold: ”International Recognition Fuels CISA Growth”. ISACA: IS Audit and Control Journal, Volume II, 1999. pp. 35-37.

[3] Gleim Irwin N., Hillison William A.: ”Auditing and Systems, Exam Questions and Explanations”, 1999. Gleim Publications, Inc., Florida, USA.

[4] ISACA: ”Chapter/University Relationships Best Practices Document”

[5] ISACA: »Control Objectives for Information and Related Technology (COBIT)«, Audit Guidelines. Information Systems Audit and Control Foundation (ISACF), USA, 2000. (www.isaca.org)

[6] ISACA: ”Control Objectives for Net Centric Technologies. Information Systems Audit and Control Foundation (ISACF), USA, 1999.

[7] ISACA: ”Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Levels”, March 1998www.isaca.org, 12.02.2001.

[8] Lucy Richard F.: ”IS Auditing: The State of the Profession Going Into the 21st Century.” ISACA: IS Audit and Control Journal, Vol. IV, 1999, pp. 44-50.

[9] Mahnic Viljan, Zabkar Natasa: ”The Role of Information System Audits in the Improvement of University Information Systems”. EUNIS 2000 Proceedings, Poznan, Poland, 13-14 April 2000, pp. 101-110

[10] McCombs Gary B., Sharifi Moshen: ”Meeting Market Needs: An Undergraduate Model Curriculum for IS Auditing”. ISACA: IS Audit and Control Journal, Volume 1, 1997, pp. 50-54.

[11] Oliver Derek J.: "Workshop on Information Systems Auditing and Control.", notes. Seventh International Conference on Information Systems Auditing and Control, Otoèec, Slovenija (24th September 1999), ISACA, Slovenian Chapter.

[12] Susnjar, Goran: ”Slovenian business managers and external IS audit: findings of the survey” (Slovenski ravnatelji in zunanje revidiranje informacijskih sestavov: izsledki raziskave). The Slovenian Institute of Auditors, Ljubljana: Revizor, 6/2000, pp. 7-26

[13] Tuck, Richard: ”Report from the Year 2000: IS Audit Recruitment”. ISACA: IS Control Journal, Volume 5, 2000, pp. 13.

[14] Wier Benson, Hurston James E., Beeler Jesse D.: ”The Impact of Higher Education and Professional Cetification on the Careers of IS and non IS auditors.” ISACA: Information Systems Control Journal, Volume 5, 2000, pp. 38-41.

[15] http://www.fri.uni-lj.si<12.02.2001>

[16] http://www.ef.uni-lj.si<12.02.2001>

[17] http://www.si-revizija.si/isaca/htm/eng/eng-030-v3.htm<12.02.2001>

[18] http://www.isaca.org/univ1.htm<14.02.2001>