Integrating IT Security Auditing to IA Curriculum

Zhixiong Chen, John Yoon and David Wang, Mercy College

Abstract – IT Security Auditing helps students understand security from management and policy perspective rather than from technological perspectives. In this paper, we brainstorm the common body of knowledge on IT Security Auditing after elaborating its importance in IA. We also share our course design and implementation from our teaching this course for the last five years to our undergraduate and graduate students in the Cybersecurity degree programs. We want to emphasize that IT Security Auditing course should be different from computer forensic courses. Lastly, we will discuss our continuing project on self-learning and self-auditing tool that is being used by our students. The results from the paper can be valuable to any universities that are thinking of offering security courses from the point of security management, policy and Information Assurance to their students in Cybersecurity or other technological majors.

Index terms – IT Security Auditing, GRC, Security Policy, Security Management

I. Introduction

Information Technology (IT) Security Auditing is increasingly becoming an important research and pedagogical topic within Information Assurance (IA) curriculum as well as security professionals because it is playing a pivotal role to ensure the security, privacy and integrity of information system that is pervasive in our workplace and personal life.

An audit is an evaluation of a person, organization, system, process, project or product. IT Auditing is an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures [1]. IT Security Auditing validates the security, privacy and integrity of information systems by collecting and evaluating evidence of an organization's information systems, practices, and operations. The goal of the audit is to express an opinion and to provide only reasonable assurance that the statements are free from material errors or log errors [2-5].

COBIT [6] is often being used as a management guideline. It provides a framework for IT governance as well as a maturity model for internal control. IT activities are defined as IT processes. A set of high level requirements for each IT process is defined as a Control Objectives or Controls. They are policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved while undesired events will be prevented or detected and corrected. Therefore, the framework provides IT Security Auditors guidelines to follow.

IT Security Auditing helps us understand security engineering, privacy and integrity from management perspective. Governance, Risk and Compliance (GRC) are the three pillars in IT Security Auditing.

To have an IT Security Auditing course integrated into IA curriculum successfully, we need to prepare students for the course, define the common or core body of knowledge (CBOK) and skills areas that we want students to possess after the class, make an assessment plan and develop rubrics for evaluation.

Since the focus of IT Security Auditing is on security management, any course dealing with IT Security Auditing should be designed to provide students security management knowledge in addition to the necessary computer-centered background, knowledge and skills. It should not be seen as another computer forensics course like hardware forensics, network forensics, application forensics or database forensics whose focus is mostly on technical details with hands on experience. The reasons we mention the difference are to tell students to apply different approach to the course, and to caution instructors who design such courses not to dive into too deep into technical details to present a whole picture of security management. We have observed at the beginning of such course that students are not that enthusiastic as in other security courses like wireless security, firewall and intrusion detection, etc. Also, we see cases from public available course syllabus or course outline in the internet that some IT Security Auditing courses are more like IT forensics courses.

In the next section, we will brainstorm the common body of knowledge on IT Security Auditing. Our goal is to show the breadth and depth of the subject as well as to give a reference model. The following two sections are to demonstrate how to design and develop IT Security Auditing class in both the undergraduate and graduate levels. We post one of our IT Security Auditing courses as an example. We also discuss the principles of designing meaningful term projects that mimic real world problems or emerging technologies. The following section is about our continuing project – a self-learning

Cybersecurity, Department of Mathematics and Computer Sciences, School of Liberal Arts, Mercy College, New York. zchen@mercy.edu

and self-IT auditing tool. This is being used by our students to advance their study and to add their project results into the tool. The last section is devoted to further discussion and practical issues from our teaching experiences during the courses for the last five years.

II. Body of Knowledge Brainstorming

In this section, we use a brainstorming chart to list the knowledge and skill areas necessities for the IT Security Auditing. The goal is to lay out them visually so that we can understand the complexity and depth of the subject. Eventually it will serve as a reference model. The brainstorming charts can also be modified easily and adapted to new situations quickly. We can use them as guidelines for course design and development. Because of the page size limitation, we have to split some charts into several sub-charts.

We start from the IT Security Auditing main domains. Each domain will be expanded in the following charts. As we see from the chart 1, IT Security Auditing is categorized into foundations, methodology and procedure, GRC, checklists and careers. The foundations cover audit, management, IT Basics, security engineering and privacy. We believe use the security engineering is more proper than just security in the context of auditing in that security is more like science while security engineering is the application of security [11].

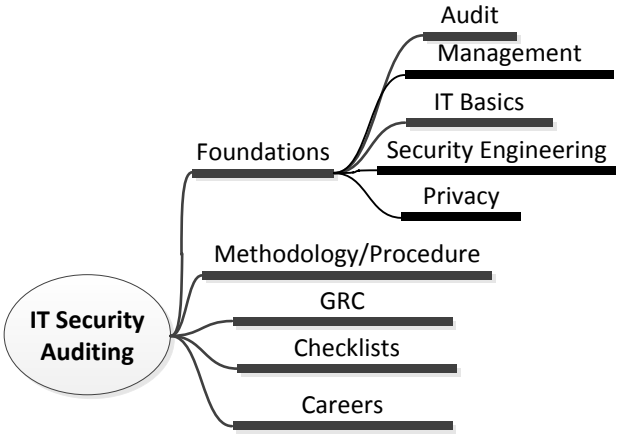

Chart 1: IT Security Auditing Main Domains

Chart 2 lists the knowledge areas for general auditing.

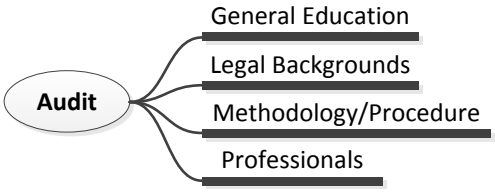

Chart 2: IT Security Auditing -> Auditing Main Topics

The general education in Audit (Chart 2) is meant to have training in speech communication, business writing and analytic skills (see Chart 3). They are crucial for an auditor to be successful. We have seen numerous examples that students with good communication skills are able to get most information from audited departments, either from managers or from team members.

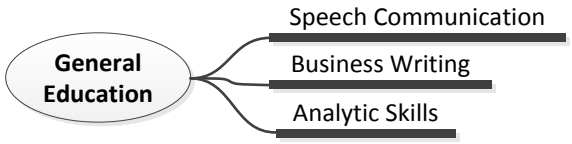

Chart 3: General Education Main Topics

The legal background (see Chart 4) of audit covers laws, regulation, standards, best practices, compliances and investigations. It also covers the general common law concepts and procedures.

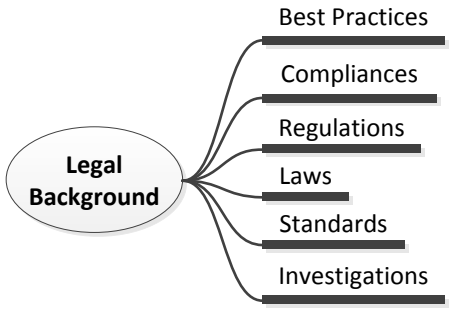

Chart 4: Audit -> Legal Background

The methodology and procedure lists auditing framework such as COSO, process, tools and principles (see Chart 5). The auditing process can be used in any auditing such as financial statement auditing, accounting auditing or a simple project auditing. They are necessary for any auditors.

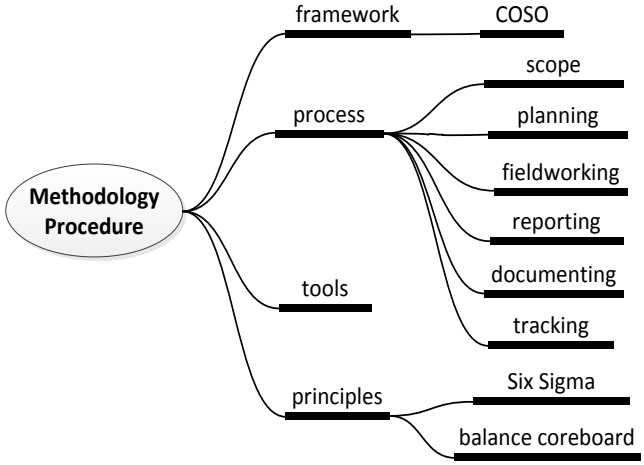

Chart 5: Audit -> Methodology and Procedure

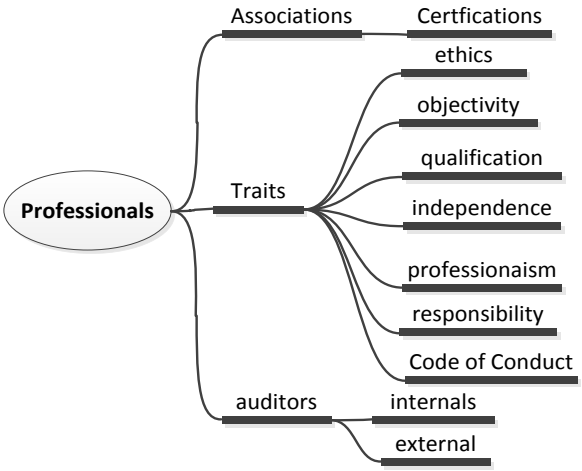

Chart 6: Audit -> Professionals

Finally, auditing professionals should have common traits such as high standard of ethics, objectivity, independence, responsibility, professionalism and qualification. To achieve these, they should follow professional code of conduct. They can be members of various auditor associations or get certifications (see Chart 6).

Chart 7 is the second foundation in IT Security Auditing, the management whose goal is to get things done.

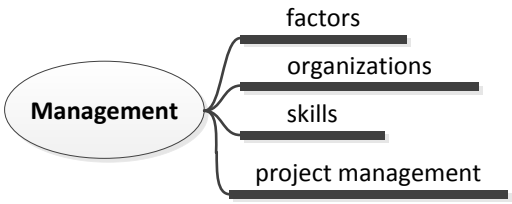

Chart 7: Foundations -> Management

Chart 8 lists the third foundation in IT Security Auditing, the IT perspective. It includes almost all subjects involved computer. They are expert domains for auditors. We expect any IT auditors should have a level of understanding of all these subjects and a level of mastering on some subjects.

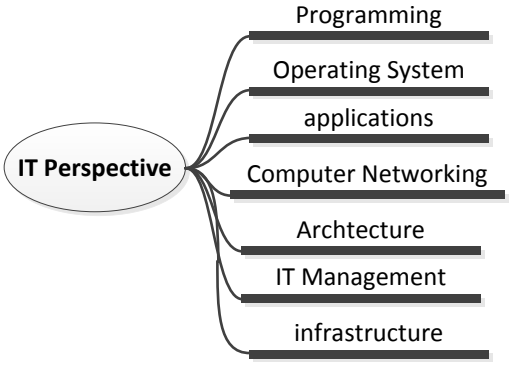

Chart 8: Foundations -> IT Perspective

We further detailed the architecture and infrastructures in chart 8 into chart 9 and 10. Various architectures are important tools to understand information systems and to connect all the isolated components together. They give us a big picture to what we want to audit. Infrastructures are another ways to get into the details. Again, we emphasize in class more on architecture, infrastructure than the detailed technical nuances.

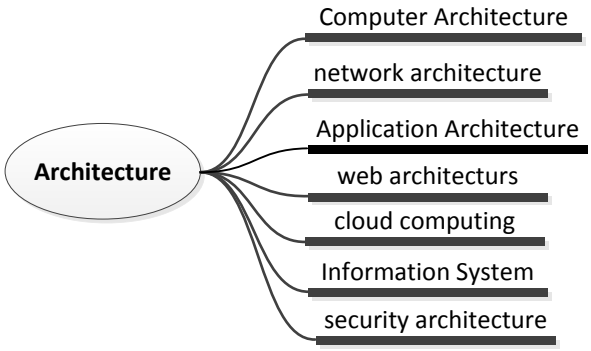

Chart 9: IT Perspective -> Architecture

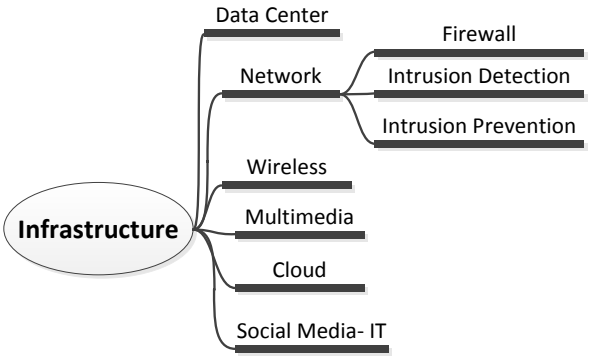

Chart 10: IT Perspective -> Infrastructure

Chart 11 is the security foundation in IT Security Auditing. Students should have a clear understanding of all these concepts and methodology, and know how to use tools to explore them.

Chart 12 lists various IT management areas such as configuration, change management, optimizations.

Continuing on the IT Security Auditing domain, we draw methodology and procedure in Chart 13, GRC in Chart 14, Checklist in Chart 15 and Careers in Chart 16.

Methodology and procedures (see chart 13) are the main topics in action in IT Security Auditing after the audit methodology and procedures (See Chart 5). It includes COBIT under framework. Many IT auditing practices follow such framework for IT process control objectives auditing as well as IT process maturity measurement. It also gives general controls that cover many important areas to be audited. Standards and regulations are also

included. Finally, the computer aided auditing tools are useful when doing auditing in systematic ways.

GRC (chart 14) are clearly unique toward IT Security Auditing. Important IA topics such as business continuity and disaster recovery are also included.

When auditing specific components or areas of information systems, auditors could use a set of well-designed questionnaires called checklists to navigate all important perspectives. This systematic approach simplifies a lot of tedious work facing IT security auditirs. Chart 15 lists common checklists. Most of them are from the book by Davis et al [5]. We also add more checklists to the list from our student projects.

Chart 16 is about IT Security Auditing careers. Built upon the auditor professionals (Chart 6), it covers the certifications and associations that can be used to demonstrate IT Security Auditing credentials.

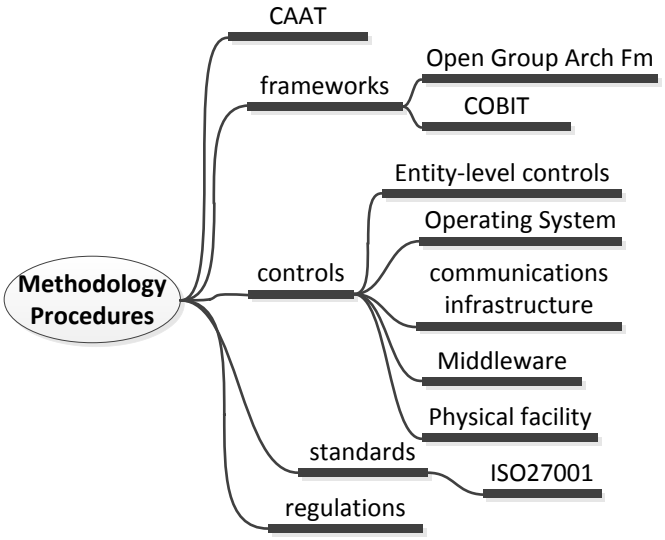

Chart 13: IT Auditing -> Methodology and procedure

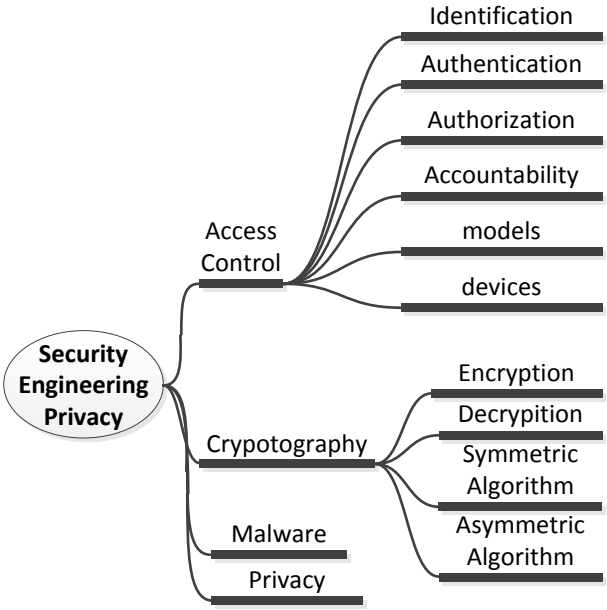

Chart 11: Foundations -> Security

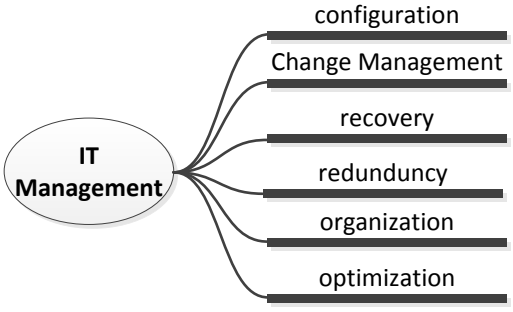

Chart 12: IT Perspective -> IT Management

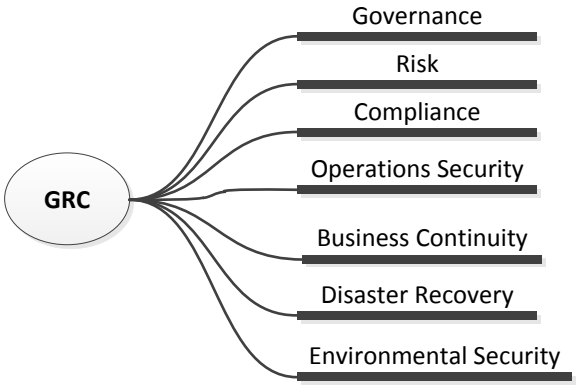

Chart 14: IT Auditing -> GRC/Management

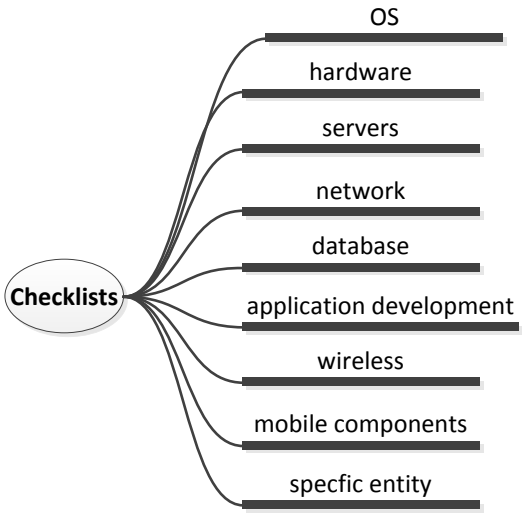

Chart 15: IT Auditing ->Checklists

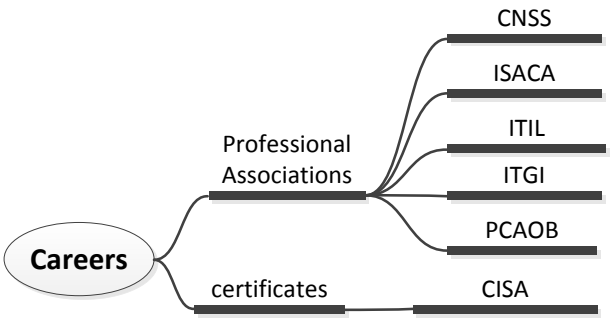

Chart 16: IT Security Auditing -> Careers

III. COURSE DESIGN

A. Host Department

IT Security Auditing courses can be offered in Business Schools because they have usually covered the auditing domain (see chart 2) and offered courses like financial auditing, risk management, public policies and similar courses. IT Security Auditing can be considered as a natural extension to their existing auditing disciplines. Currently, IT Security Auditing in most cases is still performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement. Therefore, we see a few IT Security Auditing courses are offered in Business Schools.

IT Security Auditing courses can also be offered in the criminal justice and social behavioral science departments because they have covered the legal domain (see chart 2) and human capitals, and IT Security Auditing is an extension to their legal framework.

Lastly, IT Security Auditing courses can also be offered as part of the Information Assurance and Security discipline inside Computer Science department or other technology oriented departments. They usually have covered the IT Basics (see chart 8) and offered a whole spectrum of IT that ranges from information systems to hardware, software, computer networking, operating systems and etc. IT security Auditing can be considered as an application of security and privacy to IT domains from a management angle.

Because of the different host departments, IT Security Auditing courses can have different emphasis and objectives.

B. Design Approach

Many approaches can be exploited when designing IT Security Auditing. We discuss first when IT Security Auditing is hosted inside technology departments like Computer Science Department.

One typical approach is to offer one general IT Security Auditing course that covers CBOK in more general (see chart 2 and the sub charts). The emphasis is breadth, not depth. It covers more principles, general descriptions and linkages between technology and the Audit process. In this approach, we assume that students should have all the necessary knowledge in technologies.

Another approach is focusing more on depth than breadth. It covers more specific topic and emphasizes heavily on technological details. Many technological bound students actually like this approach. It helps the actual auditing process from planning, field-working, documenting, and reporting to tracking. It also has many hands on activities that can check the actual auditing process. In this way, students gain more confidence compared to those in a general IT Security Auditing course. Students can reason and analyze the whole process rather than rely on documents provided by other experts.

But, the danger is to run such IT Security Auditing course as another computer forensics, focusing too much on cracking into the systems rather than on security management. The approach is to remind students all the time how such technical insights are being used in auditing.

For example, we have offered database security that covers only Oracle database. The instructor is able to dig deep inside out. Students are introduced to built-in processes and functionalities, configurations, internal logs and tools for log analysis and log alarm. With that deep understanding, students can apply auditing principles and practices to Oracle database and master all the nuances.

Another example is in electronic trading system auditing. We see high interest and demand, especially in the NY metropolitan area. As we know, trading is becoming more a game of high technology. High frequency trading is a new norm. A trading system that is faster due to location and computing power will have a huge advantage even if it might be just several milliseconds faster. Most trading strategies are programmed in an agile manner [7]. Sometimes these strategies are even secret from each other within a grop to avoid same strategy to be executed at the same time, which might cause a big market fluctuation. To do a better auditing job in such a complicated and sensitive IT environment, students need to be exposed to this environment first, to understand its workflow and to gain insights such as how and where to test these strategies under what scenarios. Only with such knowledge, students will be able to design a reasonable auditing process such that it does not interfere with trading operations while providing reasonable assurance of its correctness, compliance and security. Auditing data gathered from various trading stages can be analyzed offline as well as online.

When an IT Security Auditing is offered in the business department, the emphasis will be placed on the IT perspective CBOK (see chart 8 and its sub charts). The assumption is that students in the business department have enough knowledge on Auditing.

The ideal approach might be the course offered as a group teaching project which involved both faculty members from business, criminal justice and technology department.

C. Student Outcomes Assessment

The accreditation trend is moving toward student assessment and outcome based education. IT Security Auditing should design a feasible student assessment plan and set a realistic goals.

We should expect our students master the main areas of the IT Security Auditing (Chart 1), understand the general auditing process, subscribe proper methods to a new scenario, and comprehend the critical skills and methodologies used to ensure compliance to public and private sector regulatory requirements.

To achieve these goals, students should be assessed accordingly. One item in the assessing list should be a term and team project that should be an integral part of any IT Security Auditing courses. We have tried various types of projects during a period of five years, ranging from open ended projects – auditing real world problems (or domains) to close end projects - auditing simulated problems.

To do a better job in open ended projects, students usually need an insider to help them to get necessary documents and information. Without insiders, many institution or departments are reluctant to offer any meaningful data even when our students arrange for a non-disclosure legal document that states our project purpose and responsibility, and when we provide them at the end of the semester a value added auditing report. On the other hand, if students are well prepared, sometimes they can present themselves and talk through to gain access even without an insider's help. We have seen several successful projects. For example, our students went to the school library to audit its IT System that handles book loan, book return, book acquisition, inter-library book loan and user accounts. Another group successfully audited a nursing home payment system. But, open ended projects run into a same issue - quality control and time management. Students might not reach the level we would like our students to understand and to master due to the nature of the real world problems.

Closed end projects are conducted in a controlled simulated environment. A simulated company with specific IT components and infrastructure is presented to students. Students are instructed to follow steps designed by the instructor. It is easy to control the whole process, to comment on a specific area that is relevant to all students, and to grade them at the end. For example, one project asked students to audit a mock company that uses different cloud computing service deployment models. The company puts its non-essential data in a public cloud while the rest in an in-house premise. The company also adopts SaaS (software as a Service) for its rarely used commercial application software. The last piece of assumption is that some of its development work is outsourced to a company that is located in Northern Ireland.

Basically, this type of controlled projects has advantages that students can study the latest IT technology and apply IT Security Auditing skills to them. It has no existing checklist or steps that tell students how to do it. Therefore it assesses students' ability of auditing new arenas. The disadvantage is that students could not see a full picture of real world organizations, miss a chance of verbal communication and ignore many details that are usually not presented in a simulated environment.

IV. SAMPLE COURSE

In this section, we give one sample course syllabus to demonstrate how we can follow the CBOK to design and develop an IT Security Auditing within a computer science department.

It is graduate level course called IT Auditing and Compliance (IASP580). A complete course outline is posted in [8]. It falls into a category of general IT Security Auditing course. It is a three credit course. The course catalogue description is cited below:

"This course reviews the critical skills and methodologies used to ensure compliance to public and private sector regulatory requirements. It covers general auditing process and IT auditing techniques such as auditing database and data center, network infrastructure, operating systems, web applications, mobile devices, and IT projects. It introduces IT audit frameworks, standards and regulations such as COSO, CoBIT, ISO27001, Sarbanes-Oxley Act of 2002."

The course objective is "*to prepare students with critical skills and methodologies used to*

- *ensure compliance to public and private sector regulatory requirements;*
- *guarantee proper levels of controls, both IT and process level;*
- *understand audit frameworks, standards and regulations for IT environment; and*
- *gain hands on experience on governance, finance and controls."*

And the course outcome is that students are able to

- *"Understand the purpose of internal and external audit and the general audit process*
- *Comprehend critical skills and methodologies used to ensure compliance to public and private sector regulatory requirements, especially toward IT environment*
- *Apply the techniques and policies to real scenarios."*

The assessment includes online quizzes, assignments, discussion, one term project and one exam. The term projects in the Spring of 2011 includes both open ended and closed controlled projects. Students could choose whatever they want to fit their interests. In addition, some students were offered to do a coding project that is able to put checklists we developed into an online system that can be referred by students in the future.

The final note is that we can also find such course offered in another department. Just for comparison, without exhaustive search, I find one IT Security Auditing course offered at Georgia State University inside the School of Accounting [9]. The course objectives are

- *"Develop assurance objectives for risks of information systems.*
- *Design assurance procedures.*
- *Implement assurance procedures with software tools.*
- *Communicate assurance results.*
- *Collaborate with others to achieve these objectives."*

V. Self-Learning and Auditing Tool

For the last two years, we have been developing a self-learning and self-auditing tool that provides students a common platform for their term projects. First, it is a repository that stores student projects' results in the form of auditing checklist questions accompanied with relevant documentations. Students can refer to these checklists for self-study and prepare their own projects. They can make modifications to enhance existing checklists. The documents present specific knowledge area with links and conference and journal articles. We have experimented to search results from just these links using our own search engine. The results are more relevant to IT Security, focused and creditable compared with the search results from search engines like google or bing. Lastly, it is also a point that we can start various monitoring tools, mostly open sources projects like wireshark, nmap.

Figure 1 and 2 are screenshots of the tool. We have categorized checklists into two portions, technological domain and entity domain. The Entity domain could be student working places, primary care physician, student account, a public library, a convenience store, a gas station, church or a nursing home. The technological domains can be Linux, MS Windows, wireless, mobile, Window Active Directory, server side scripting languages, password, firewall, databases, computer network, etc. They can be used by any entity domain.

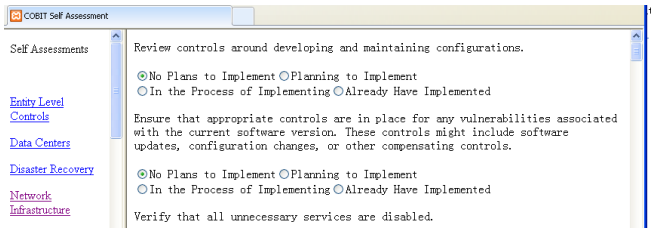

Figure 1: IT Security Auditing Tool Screenshot - checklist

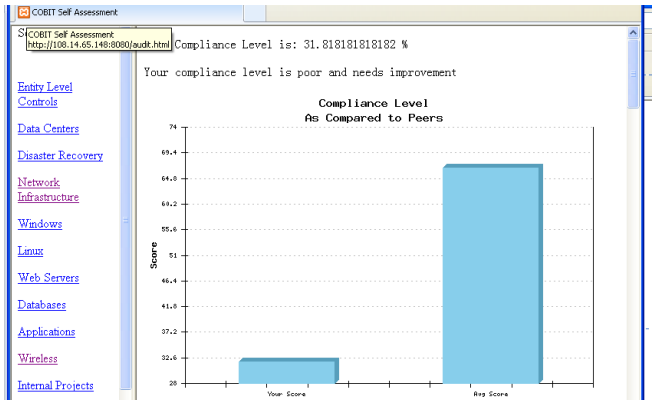

Figure 2: Embedded Application in Tool – maturity model

VI. Discussion

Students are benefiting from exposure to IT Security Auditing. They study security from management to techniques. Many students go on to have master's projects on topics related to security policy, practice, real world problems, and GRC. It gives students another option based on their technological background and career interests.

Such security management exposure also helps student in their careers and employment. More and more private institutions on addition to government agencies and public traded companies realize the importance of IT security auditing thanks to the publicity of security issues in the public media. US Department of Labor's Occupational Outlook Handbook [10] describes "Computer security specialists plan, coordinate, and maintain an organization's information security. These workers educate users about computer security, install security software, monitor networks for security breaches, respond to cyber-attacks, and, in some cases, gather data and evidence to be used in prosecuting cybercrime. The responsibilities of computer security specialists have increased in recent years as cyber-attacks have become more sophisticated". It projects employment under the IT category to "grow much faster than the average for all occupations and add 286,600 new jobs over the 2008-18 decade". Hence, we need to prepare all rounded students to meet the challenges.

VII. REFERENCES

[1] CNSS (The Committee of Natioanl Security Systems, http://www.cnss.gov), digital publication (CNSSI-4009) at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf, accessed on February, 2012.

[2] Zhixiong Chen, Jong Yoon, Christopher M. Frenz, Kenneth Compres, IT Governance, Compliance and Auditing Curriculum – A Pedagogical Perspective, In the proceedings of the 7th IEEE World Congress on Services, July 4-9, 2011, Washington DC, pp414-421

[3] Carlin, A. Gallegos, F., IT Audit: A Critical Business Process, Computer, 2007, VOL 40, pages 87-89

[4] Sandra Senft and Frederick Gallegos, Information Technology Control and Audit, 3rd Ed, 2009, Taylor & Francis Group CRC Press

[5] Chris Davis, Mike Schiller and Kevin Wheeler, IT Auditing, Using Controls to Protect Information Assets, McGraw-Hill, 2006

[6] ISACA (Information Systems Audit & Control Association, http://www.isaca.org), digital publication, COBIT4.1 (The Control Objectives for Information and related Technology), at http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx. accessed on March, 2011. Note: COBIT now is under the responsibility of ITGI (The IT Governance Institute, http://www.itgi.org/).

[7] Interested in trading strategy can refer to http://en.wikipedia.org/wiki/Algorithmic_trading as a starting point.

[8] IASP580: IT Auditing and Compliance, https://www.mercy.edu/academics/school-of-liberal-arts/department-of-mathematics-and-cis/information-assurance-education-center/ias-education/

[9] http://www2.gsu.edu/~wwwsys/ac863.htm, Accounting 8630 IT Auditing, School of Accountancy, Georgia State University.

[10] US Department of Labor's Occupational Outlook Handbook , 2010-11 edition, http://www.bls.gov/oco/ooh_index.htm

[11] Ross Anderson, Security Engineering, A Guide to building Dependable Distributed Systems, 2nd Ed., Wiley Publishing Inc., 2008