IS 681: Computer Security Auditing

Fall; September 6, 2016 – December 14, 2016

Please refer to online syllabus for detailed assignments.

Office Hours: Fridays 5-7PM, EST, by appointment

Course number, title, credits

IS 681 Computer Security Auditing. (3 credits)

Textbook

IT Auditing Using Controls to Protect Information Assets by Chris Davis and Mike Schiller
Publication Date: **January 10, 2011** | ISBN-10: **0071742387** | ISBN-13: **978-0071742382** | Edition: **2| McGraw-Hill**

Catalog Description:

This course reflects the current emphasis on information security and security management in Fortune 500 corporations. Students will delve into information protection concepts, privacy impact analysis, computer crime, legal issues, controls and auditing systems, and firewall configuration. Students will have the opportunity to learn and perform evaluations on security infrastructures in a controlled environment in class labs by completing realistic security auditing projects and using vulnerability assessment tools to assess risks and evaluate security controls on networked infrastructures.

http://catalog.njit.edu/graduate/computing-sciences/information-systems/#coursestext

Method of Instruction

The method of instruction will combine the following elements:
- Online Class Discussion, Collaboration, Forensic Research Analysis and Report
- Forensic Research Presentation, Project Paper Deliverable

Policy on Paper Submission

Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. Please note that life emergencies happen. Do NOT wait until the last moment to start on your paper. If you do that and something comes up to impede your progress, it will hamper your ability to turn in your paper on time. Papers MUST be submitted electronically via Blackboard.

All papers must include the following statement:
"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____"

Reading Assignments:

The scope of this course is very broad, and a large amount of reading is required. However, the relative importance of materials, as specified in the course outline, varies. Specifically assigned materials must be read in detail. Materials to which students are directed or for which copies are provided but which are not specifically assigned are recommended for added understanding of required material, but are optional in the sense that students will not be held explicitly responsible for anything that appears only in these materials. They are appropriate either for students who have difficulty with the subject matter based on the required readings or for those who want a deeper understanding of the material. Recommended

background reading is valuable for overall understanding, may provide a technical depth beyond the requirements of the class, may provide valuable material for student research topics, and may be useful in responding to comprehensive essay questions.

Since much of what is happening in information security is happening now, current events will play a role in class discussions. As professionals, it is crucial for you to keep up with events as they unfold. There is no substitute for regular reading of business and technology news in a major newspaper, for following current journal articles, visiting key web sites, and for noting the direction of industry organizations such as the IEEE, IETF, and the ACM. You should constantly consider how what you read in such sources fits into the subject you are studying. Current articles, including Web articles, may be assigned as supplementary reading as the course progresses.

Students are encouraged to use as many and varied sources as possible in exploring the questions presented during the course, and to share those sources with their classmates. References to sources should be explicit in exchanges among the students and instructor, and will be considered in determining the extent to which each student participated for purposes of awarding grades.

Grading Policy:

The overall course grade will be established as follows:

Grading Criteria	Percentage
Computer Security Audit Research Project Paper	30
Computer Security Audit Research Project Presentation Slide Deck	10
Discussion Participation	30
Final exam	30
Total	**100**

Course Topics:

- Build and maintain an internal IT audit function with maximum effectiveness and value
- Audit entity-level controls, data centers, and disaster recovery
- Examine switches, routers, and firewalls
- Evaluate Windows, UNIX, and Linux operating systems
- Audit Web servers and applications
- Analyze databases and storage solutions
- Assess WLAN and mobile devices
- Audit virtualized environments
- Evaluate risks associated with cloud computing and outsourced operations
- Drill down into applications to find potential control weaknesses
- Use standards and frameworks, such as COBIT, ITIL, and ISO
- Understand regulations, including Sarbanes-Oxley, HIPAA, and PCI
- Implement proven risk management practices

Computer Security Audit Research Project Paper and Presentation Slide Deck

The student will research a real-world case such as the Stuxnet worm attack, and create an audit report. Your audit report must include detailed technical background and how the threat compromised the target. Your presentation slide deck will include a summary of your findings. The research paper could be in 10-15 pages of double spaced.

Week	Date	Discussion Topic	Assignments
1	9/6	Build and maintain an internal IT audit function with maximum effectiveness and value	Read Text Discussion Post
2	9/13	Audit entity-level controls, data centers, and disaster recovery	Read Text Discussion Post
3	9/20	Examine switches, routers, and firewalls	Read Text Discussion Post
4	9/27	Evaluate Windows, UNIX, and Linux operating systems	Read Text Discussion Post
5	10/4	Audit Web servers and applications	Read Text Discussion Post

6	10/11	Analyze databases and storage solutions	Read Text Discussion Post
7	10/18	Analyze databases and storage solutions	Read Text Discussion Post
8	10/25	Assess WLAN and mobile devices	Read Text Discussion Post
9	11/1	Assess WLAN and mobile devices	Read Text Discussion Post
10	11/8	Audit virtualized environments	Read Text Discussion Post
11	11/15	Audit virtualized environments	Read Text Discussion Post
12	11/22	Evaluate risks associated with cloud computing and outsourced operations	Read Text Discussion Post
13	11/29	Drill down into applications to find potential control weaknesses Use standards and frameworks, such as COBIT, ITIL, and ISO Understand regulations, including Sarbanes-Oxley, HIPAA, and PCI Implement proven risk management practices	Read Text Computer Security Audit Case Study Research Project Presentation Slide Deck Due
14	12/6	Drill down into applications to find potential control weaknesses Use standards and frameworks, such as COBIT, ITIL, and ISO Understand regulations, including Sarbanes-Oxley, HIPAA, and PCI Implement proven risk management practices	Computer Security Audit Case Study Research Project Paper Due
15	**12/13-12/14**	Final Exam. Please note this end date as no assignments will be accepted after this final date.	**Ends on 12/14**