



COURSE SYLLABUS

IA 532: Audit Controls in Information Security

Instructor: _____

Office Hours: _____

Office: _____ **Telephone:** _____ **FAX Number:** _____

Internet/E-Mail Address: _____

Opening Statement: This document is meant to serve as an information statement for your reading and use for this course. It also serves to identify timelines, requirements etc. The instructor reserves the right to make any additions/deletions or changes to this document or course as deemed necessary.

Course Description: A course for the information system security professional, emphasizing the audit and control of information systems. The course follows the curricula recommendations of the Information Systems Audit and Control Association (ISACA) and the Information Systems Audit and Control Foundation (ISACF), and uses the Control Objectives for Information and Related Technology (COBIT) as its instructional framework.

Course Prerequisites/Corequisites: IA 542, IA 543

Course Objectives: Upon successful completion of this course, students should be able to:

1. Understand basic information systems management
2. Work within the basic framework of auditing practice and theory
3. Understand the applicable legal, standards, policy and regulatory environment for information systems
4. Understand risk management principles as applied to information systems
5. Use various techniques for information system vulnerability assessment
6. Apply general audit practice to information systems
7. Have a comfortable understanding of how information security professionals work with and support IT auditors within their organizations

Student Requirements: The overall goal of this course is to prepare IA professionals with a basic grounding in IT audit and control processes so that they may work productively with IT auditors within their organizations. The highest level of student gain will be achieved by participation in the team-based directed exercise(s) and by participation in classroom activities as well as individual assignments. Each student will be required to actively participate in the class exercises and contribute to the overall team effort. Students will be given reading assignments as well as assigned written projects.

Text and Handouts: Students will receive reading assignments that may include handout material, and/or research searches, and are responsible to read and act on the material as directed.

- Primary Text – Auditing Information Systems Champlain, Jack J., pub John Wiley & Sons, 2003, ISBN 0-471-28117-4
- COBIT Executive Summary
- COBIT Framework
- COBIT Control Objectives
- COBIT Management Guidelines
- COBIT Implementation Tool Set

Assessment and Evaluation: The final grade for the class will be based on the following requirements as directed by your instructor:

- Team based development, presentation and evaluation of a final project, including a complete bibliography, and areas of further research will account for 40% of each student's grade.
- Student participation in class activities and individual assignments will account for 20% of the student's grade.
- Mid term and final exams will account for 20% each of the student's grade

All points are cumulated, converted to percent form, and converted to letter grades based on this straight scale: 94% and above, A; 90% and above A-; 87% and above, B+; 84% and above, B; 80% and above, B-; 77% and above, C+; 74% and above, C; 70% and above, C-; 67% and above, D+; 64% and above, D; 60% and above, D-; below 60%, E.

Notes on Requirements and Grading:

- Class sessions will involve interactive approach and student activities. Students are expected to have textbooks and other assigned materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, or other misc. materials including disks, or backup files (in case a file is lost or damaged).

Attendance at all times is required of all students, and failure to attend is considered lack of participation. Verifiable emergencies will only be considered.

General Policies:

- Attendance and punctuality is mandatory. Class will start at the given time.
- All cell phones, pagers and any other miscellaneous forms of communication must be turned off prior to the start of class and remain turned off until after class is completed. This is out of courtesy for the other students and to insure an un-interrupted class.
- Speak to the instructor as needed.
- Students should comply with expectations for use of the college and university laboratories and classrooms, with standards for fair information practices, and with licensing provisions of the software in use.
- Students must complete their own work when given an individual assignment. During team-based assignments they will work with one another to solve problems and develop the team-based project. Students who submit the work of other students, including companies and organizations, as their own (Plagiarism), will be penalized to the full extent permitted by University policy.
- Late work is not accepted. Oral presentations may not be made up.
- Inability to prepare for an assignment and poor time management are not considered valid reasons for late work or re-scheduling. In addition, students must back up work, for lost disks or damaged files is not sufficient reason for extensions.
- Class sessions may involve some lecture, Caucus/Online, with mostly group-facilitated activities. Therefore, it is the student's responsibility to have completed the scheduled reading assignment prior to the class session. The student must also complete the assigned chapter activities/projects during scheduled class sessions. Active listening is also part of learning. Students are expected to have textbooks and other needed materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, and/or other materials.
- Be prepared to conduct discussions online through Caucus or another form of online viewing such as e-mail.
- Students are expected to complete all assignments in a neat, accurate and professional manner; otherwise, materials will not be accepted. This includes the word processing of all assignments with spell checking and proofreading mandatory. This also includes stapling your materials if needed so they do not become loose.

- All assignments will be graded for compliance to the author's directions.
- Final grades will not be given in person, by telephone, e-mail, fax or any other communications median except that of University standard written grading at the end of the semester.
- Attendance/participation is required therefore it is the student's responsibility to obtain all missed instruction from another class member. The instructor will not repeat instructions or demonstrations for any student missing class. Keep in mind that attendance is mandatory.
- A grade of "I" will be given only in accordance with Eastern Michigan University's Graduate school guideline.
- By University policy the instructor has the option of failing a student who does not attend class on the day of the final examination set by the university. Attendance at final periods during which students are presenting their work is required of all students and failure to attend is considered lack of participation.

Course Content and Schedule: This schedule is an approximate timeline for the student.

Week 1

- **Introductions**
- **Course Review and Intro**
- **Principles of Information Systems Management as Applied to the It Audit Environment**
- **Auditing Practice and Theory**

Week 2

- **Legal, Regulatory, Standards and Policy Environment of Information Systems**
- **Security and Privacy in Information Systems**

Week 3

- **Project and Team Selection**
- **Information Systems Audit Approach**
- **Physical, Logical and Environmental Considerations**

Week 4

- **Introduction to COBIT**

Week 5

- **COBIT Continued**

Week 6

- **Vulnerability Assessment and other IT Audit Tools**
- **Vulnerability Assessment Lab**

Week 7

- **Mid Term Exam**

Week 8

- **Risk Management Principles and Techniques**

Week 9

- **Security Certifications (SAS 70, TruSecure, etc.)**
- **Project Management Controls**

Week 10

- **Digital Forensics as an Audit Tool**

Week 11

- **Relationships Between Information Security and IT Auditing teams**
- **Preparing for an IT Audit**

Week 12

- **Introduction to Information Systems Security Incident Investigation**

Week 13

- **Project Work Session**

Week 14

- **Team Project Presentations and Business documents turned in.**
***No late projects or presentations will be accepted.

Week 15

- **Final Exam**

Overview of the Semester Project:

Grading: There are 40 points for the semester project and presentation.
There are 60 points for participation in class activities, assignments and exams.

The final project will be developed in teams with a team leader giving an oral presentation of the project to the class. Each student will write a portion of the team report and will be responsible for his or her contribution to the overall project. Each team will provide a final written team report with each team member's contribution identified individually.

More on Planning the Project:

Each team will develop a word processed business document, **completed in APA or MLA format**, which will be presented using PowerPoint and will at minimum include the following:

- Cover page with all Team Members Names, etc.
- Table of contents
- Names of Team members and their individual responsibilities
- The Team Leader is responsible for submitting each team member's participation and contributions to the project, which is to be included in the final document package.
- Statement of the problem. What are the issues you are dealing with and why.
- Summary statement focusing on the organization.
- Solution Statement: How will you deal with the problems, issues, etc.
- Bibliography
- Areas of further research, including a preliminary research proposal on a significant information security problem related to Systems Auditing.

The focus of the final project is to design and develop a report for Senior Management that demonstrates the implementation of system audit controls necessary to maintain the confidentiality of records while allowing the records to be available to a user. The project will focus on the auditing concepts presented in the course. Each groups report will focus on system compliance and the evaluation of the current systems in place.

You will need to use NON-CONFIDENTIAL data for your project. Please do not UNDER ANY CIRCUMSTANCES use data that would breach any confidentiality. Fictitious companies and or organizations will only be used.

