

MGA 610 Information Systems Audit syllabus

Course Description

This course presents information systems audit and control concepts and management practices. As business continues towards a more substantial reliance upon the capabilities of information systems, it becomes increasingly important for auditors to understand information systems and how they relate to financial and general organizational controls. Upon completion of this course students will be able to conduct audits of information systems. This course presumes prior exposure to general audit concepts and a general knowledge of information systems.

Required Background

This course is about information systems (information technology) auditing and controls. Students are expected to have some familiarity with computer systems, networking concepts, and application development processes. From that basic understanding you will learn how to audit these systems, filling in details about specific IT concepts and practices as necessary to understand how to audit a particular area.

Course Objectives

Understand the role of the IS auditor and the IS audit function. Understand the purpose of controls in an information systems environment. Learn how access to systems, resources, and data can be controlled. Assess the design, placement, and quality of controls. Understand some of the basic theory underlying computer security policies, models, and problems. Learn models for dealing with risk. Understand the basic issues in auditing computer security policies and mechanisms.

Instructors Teaching Philosophy

The most effective learning experiences are those in which the student is fully engaged. Class is structured and graded to encourage constructive class participation through a variety of learning experiences, in-class and out-of-class group work, project(s), online work, and quizzes and exams.

Instructors Office Hours

Office hours are on the same day as the course, immediately following class. If this time conflicts with your other courses or your job work hours, appointments are available outside of normal office hours.

I encourage students to utilize office hours for clarification of class material, reading material, and other questions related to class. I also encourage you to see me if you have a career interest in the area of IT audit, IT security, or risk management.

Grading

	Undergraduate Points Available	Graduate Points Available
Assignments	15	15
Discussion, work and quizzes In class – 10 points Online – 10 points	20	20
Projects Audit pre-work – 5 points Audit report – 20 points	25	25
Midterm	15	15
Presentation (Graduates Only)	-	10
Cumulative Final	25	25
Total	100	110

Projects

Projects are group work and a significant portion of your grade. Projects will require working with area companies to perform a general audit. This will include travel to the offices of the companies. Groups are responsible for identifying the company that they wish to audit and for making arrangements with that company. Groups that do not identify a company on their own will have a company assigned to them. Grades are given based on work products, group performance, and individual contribution.

Exams

Material for exams will be taken from a variety of sources, including assigned readings and research, homework assignments, and class lectures. The midterm will be given and grades will be returned before the last day to drop the course with an “R”. The final exam is cumulative.

Course Policies

Late Assignment Policy

If you turn in an assignment past midnight on the day that it is due, the highest grade that you can receive is the lowest grade of everyone who turned the assignment in on time.

Academic Dishonesty Policy

Questions about academic dishonesty should be directed to the course instructor. All cases of academic dishonesty will be submitted to the department and the University for appropriate action. All assignments that contain academic dishonesty will receive an automatic zero grade and may jeopardize the student’s grade for the whole class.

It is suggested that you read <http://www.indiana.edu/~wts/pamphlets/plagiarism.shtml> before completing any assignments.

1. Purpose and value of IS audit and IT governance
2. Organizational Responsibilities
 - a. Executive management
 - b. Auditors
 - c. IT and Information security
 - d. General users
3. Information security
 - a. Three primary goals (confidentiality, integrity, availability)
 - b. Principles: Accountability, Awareness, Ethics, Multidisciplinary, Proportionality, Integration, Timeliness, Assessment, Equity
4. Ethics and legal issues
 - a. Agreements for: confidentiality, trade secrets, discovery, non-compete
 - b. Intellectual property and fair use
 - c. Patents, trademarks, and copyrights
5. Audits and Assessments, Major Guidance
 - a. Differences between an audit and an assessment
 - b. Guidance and where each guiding document is applied
 - i. GAAP
 - ii. SAS: SAS 48, SAS 70, SAS 78, SAS 94
 - iii. COSO
 - iv. COBIT
 - v. For COBIT, be able to describe and indicate how the following are used: Process objectives, Information criteria, IT Resources, Maturity Models, Critical Success Factors, Key goal indicators, Control objectives
 - vi. ITIL
 - vii. ISO17799
6. Risk
 - a. Business risk, audit risk, security risk, continuity risk
 - b. SEI risk statement (two things needed to express risk clearly)
 - c. Components of risk: threat, vulnerability, exposure, impact, consequence
 - d. Risk response options: manage, reduce, transfer, ignore, monitor
 - e. Threat classes: natural, accidental and unintentional, intentional, political unrest, acts of war
 - f. Threat agents, threat agent motives
 - g. Four basic steps to a risk assessment
7. Information security programs
 - a. Relative importance of people, policy, and technology
 - b. Program foundation: policy, education, ownership, defined responsibilities
 - c. Role of risk management in information security programs
 - d. Program components: charter, risk assessment, data management, access management, technical architecture, incident response, DR/BC, physical security, sanction
 - e. Key department relationships and their purpose: human resources, training, risk management, quality management, compliance, executive management

8. Information Security Management
 - a. Supporting role and purpose of: policy, training, culture, baselines, system acquisition and development, change management, configuration management, monitoring, personnel policies, assessments, metrics, and evaluation
 - b. Incident response and basic steps: identification, containment, collection, recovery, analysis
9. Policy, process, and procedure
 - a. Differences between policy, process and procedure
 - b. Purpose of policy, process and procedure
 - c. Be able to identify policy meta-data
 - d. General understanding of what should be addressed by policy:
 - i. Program charter, risk management, acceptable use, data management, physical protection, access management, personnel security, sanction, incident response, IT management
 - e. Preferred / most effective policy authors and creation processes
10. Organization
 - a. Basic job responsibilities of various IT functions, particularly:
 - i. Programmer, programmer/analyst, systems analyst, database administrator, systems project manager, project manager, quality analyst / tester, network administrator, system administrator, voice and data communication analyst, web content administrator, webmaster, hardware technician, help desk specialist, security specialist, operator, IS auditor, CIO
 - b. Various ways of organizing an IT department, and advantages and disadvantages
 - c. How size impacts ability to segregate duties
11. Software / System Development Life Cycle
 - a. Four basic steps in SDLC: analysis, development, testing, implementation
 - b. General sense for SDLC risks (don't have to know each bullet on slides)
 - c. Differences between pre- and post- implementation audits
 - d. Pre-implementation: approaches, role of auditor, advantages, disadvantages
 - e. Post-implementation: approaches, role of auditor, advantages, disadvantages
12. Application development
 - a. Architectures and placement of controls
 - b. Role of databases in control design
 - c. Database issues
 - d. Input, output, transaction controls
 - e. Virus, trap door, Trojan horse, logic bomb, worm
 - f. Time of check / time of use
13. Networking
 - a. Concept of layering (OSI model, TCP/IP – no detail needs to be memorized)

- b. Concept of encapsulation (wrapping of packets as they go down the stack, and unwrapping of packets as they go up the stack)
- c. General sense of what the following are: LAN, CAN, MAN, WAN, VPN
- d. General difference between circuit-switched and packet-switched networks
- e. LAN topologies: star, bus, ring
- f. Network devices: hub, bridge, router, gateway
- g. Network protection mechanisms, and what they do:
 - i. firewalls, proxy servers
 - ii. intrusion detection systems
 - iii. SSL
- h. Network attacks:
 - i. Spoofing, denial of service, sniffing, session hijacking

14. Controls

- a. preventative, detective, deterrent, corrective, recovery
- b. Administrative, Technical, Physical

15. Audit planning

- a. Scope, objectives

16. Audits vs. assessments

17. Facilities security and environmental controls

- a. Human safety factors
- b. Media and asset control
- c. Physical access controls
- d. Surveillance Monitoring
 - i. Card / biometric
 - ii. CCTV
- e. Alarms
- f. Administrative response
- g. Power
 - i. UPS and generator loading
 - ii. Emergency power-off
- h. HVAC
- i. Fire detection and suppression
 - i. Placement of smoke / fire detectors
 - ii. Fire extinguishers
 - iii. Fire suppression systems
 - 1. Types – dry and wet pipe, FM-200 or HFC-227, Halon 1301 replacements
 - 2. Design – delay, by-pass
- j. Liquids
- k. Data center location and design
 - i. Placement relative to exterior walls,
 - ii. Windows
 - iii. Auxiliary doors
 - iv. Traffic patterns
 - v. Raised floor (and construction of walls)

18. Questions from the Graduate Presentations