THE UNIVERSITY OF TEXAS AT AUSTIN ACC F380K 12 - COMPUTER AUDIT AND SYSTEM SECURITY: COMPLIANCE AND ADVISORY PERSPECTIVES

Summer 2013 Unique#: 71370

VERSION: 6/3/2013

Instructor: Huseyin Tanriverdi

Class times : Monday / Wednesday 1:30-5:30 p.m.

 Class location
 :
 UTC 4.122

 Instructor's Office
 :
 CBA 5.208

 Phone
 :
 (512) 232-9164

 Fax
 :
 (512) 471-0587

E-mail : <u>Huseyin.Tanriverdi@mccombs.utexas.edu</u>

Office Hours : By appointment

Teaching assistant: Kui (Andy) Du, <u>Kui.Du@phd.mccombs.utexas.edu</u>

Course objectives:

This course makes an introduction to information technology (IT)-related risks of organizations, IT governance and control frameworks, and IT audit and advisory services aiming to reduce IT-related business risks and increase returns of organizations. IT has become a critical enabler and transformer of business innovation, growth, and profitability across almost all sectors of the economy. IT has also exposed organizations to greater risks. Academic and practitioner literatures are fraught with cases showing how misalignment of IT and business strategies, inadequate investments in IT, failures in IT implementations, glitches in IT operations, or IT security breaches can significantly affect the confidentiality, integrity, and accessibility of information assets, disrupt business operations, lead to financial losses, and cause damage to reputations of organizations. Pervasiveness of IT systems across value chains and business networks of organizations increases the importance of IT-related controls. Regulations such as the Sarbanes-Oxley (SOX) regulation of 2002 require top executives of public companies to be directly responsible for IT-enabled internal controls that impact financial statements of their companies. Thus, it is important for business leaders to understand how they can minimize risks and maximize returns of IT to obtain more favorable risk-return positions for their organizations. This course aims to equip students with an understanding and appreciation of the following topics:

- IT environments, IT functions, IT assets and terminology of organizations
- Different types of business and IT risks faced by organizations
- The roles of IT in risks, returns, and risk-return trade-offs of organizations
- Governance and control frameworks that aim to mitigate IT-related organizational risks
- IT audit process, generally accepted IT audit standards, frameworks, and methodologies
- IT general controls, IT application controls, identity governance and access controls
- Data privacy controls
- Security governance
- Computer Aided Audit Tools & Technologies (CAATTs)
- IT audit and advisory services provided by the accounting industry
- IT-related risks and mitigation approaches in corporate outsourcing, merger, acquisition, divestiture, spinoff, and split-up transactions
- Professional organizations and certifications relevant to IT audit and security

Course delivery format:

The course material is delivered through lectures, guest speakers, case discussions, and hands-on application assignments. Students are encouraged and expected to participate actively in class discussions and presentations. They are expected to read and analyze assigned reading articles, cases, and lecture and guest speaker notes in advance of class and come to class prepared for discussions. Through participation in class discussions, students control and share the responsibility for learning.

Course website:

Hosted on the Blackboard system http://courses.utexas.edu/. Login using your UT EID and select ACC F380K.12. Updates to this syllabus and other course materials will be posted on this website. Please log on to the site before each class to view the announcements and assigned materials.

Required cases and reading materials:

Required cases and reading materials for each session are listed in the course schedule below.

- (HP): Harvard Business School cases and articles that we will use in this class are available in a digital Harvard Package (HP), which can be purchased online from Harvard Business School Publishing at https://cb.hbsp.harvard.edu/cbmp/access/19787199
- Non-Harvard cases and readings will be available on Blackboard.

Grading:

Contributions to in-class discussions	:	20%
CAATTS Assignment	:	20%
Case write-up	:	20%
Take home final exam	:	40%
Total	:	100%

Contributions to in-class participation (20%). This class relies significantly on case discussions and guest speaker presentations. Students are expected to actively contribute to the learning of their peers by asking relevant questions, making relevant comments, and sharing their own perspectives on issues being discussed in cases and presentations. Attendance is required, but it earns only 20% of the in-class participation credits. The remaining 80% of the in-class participation credits can be earned by making contributions to discussions in the classroom.

There is no substitute or make-up for earning in-class participation credits. Requests to do extra work in lieu of participation will be automatically declined. If you miss the opportunity to contribute to in-class discussions in a session, you can try to make up for it by increasing your participation levels in other sessions you are able to attend throughout the semester. Your final participation grade will be assigned based on your participation patterns throughout the semester.

Advanced preparation for in-class discussions would help you make substantive contributions to in-class discussions. You are expected to read, analyze, and think about the assigned readings, cases, and other lecture materials before coming to class. This preparation is likely to increase your ability to make substantive contributions to in-class discussions and earn participation credits.

Please consult the following note in the Harvard Package (HP) for guidance on how to prepare for a case discussion: Ellet, W. "How to Discuss a Case" Chapter 8 of "The Case

Study Handbook: How to read, discuss, and write persuasively about cases. Harvard Business Press," Product#: 2450BC-PDF-ENG, Apr 17, 2007, pp. 1-12.

The following factors will contribute positively to earning in-class participation credits:

- Doing assigned readings and cases and coming to class prepared for discussing them
- Arriving before the start of class and staying until the end
- Listening actively to your peers, instructor, and guest speakers
- Asking relevant questions
- Linking and synthesizing topics covered throughout the semester
- Bringing to discussions examples and questions from your prior work experiences
- Synthesizing or reconciling issues being discussed
- Responding to questions
- Disagreeing with others constructively
- Neither dominating the conversations nor being too quiet
- Exhibiting a good sense of humor

Using a name card and sitting roughly in the same place each class will help instructor and other students better recognize your contributions.

CAATTS Assignment (20%): You will work on a team assignment to gain hands-on experience with one computer assisted audit tool, namely ACL software. This software is available in business school labs. Course TA will provide a tutorial on ACL on June 24th in the Mod Lab, as listed in the course schedule below. After this tutorial, you will be given a CAATTS team assignment. You are asked to form a 4 or 5 person team and inform the course TA about your team members as soon as you can but no longer than the end of the ACL tutorial on June 24th.

Case write-up (20%): We will discuss several cases in this course. Case #3 "Security breach at TJX" on June 19th is a required write-up case. Write-up and discussion questions for this case will be posted on the class website. Your write-up should address the assigned questions by utilizing course concepts and analyzing case facts and issues. The managerial issues entailed in the cases are open ended. They can potentially be analyzed and addressed in multiple different ways. This case write-up is an INDIVIDUAL assignment. You should analyze the write-up case yourself and develop your own unique answers to the write-up questions. Submissions that indicate that the author developed the answers in communication, cooperation, or collaboration with anyone else will be subject to the scholastic dishonesty policies of the University referenced in the syllabus. This case write-up is due by 1:30pm on June 19th. Submissions after the deadline will not be considered. There will be no make up for missed submission except in documented medical emergencies./ Case write-up, format, submission, and grading guidelines will be posted on the course website.

Take home final exam (40%): A take home final will be given at the conclusion of the semester on July 10th. This final is cumulative of all material covered throughout the semester. It will be given by 5:30pm on July 10th and returned by 5:30pm on July 13th in the digital drop-box of the Blackboard course management system. Late submissions will incur a deduction of 10 points for each hour of lateness after the due time.

Final letter grades: Weighted average of all grade components will be used in assigning final letter grades. If the class average turns out to be below 90, letter grades will be assigned based on a curve. The curve will not have predetermined percentages. Breaks in grade distribution will be used in setting letter grade boundaries. If the class average turns

out to be 90 or above, the following table will be used in converting weighted grade averages to final letter grades.

Grade conversion table to be used if class average is 90 or above		
Range of weighted grade average	Letter grade	
95-100	Α	
90-94	A-	
85-89	B+	
80-84	В	
75-79	B-	
70-74	C+	
65-69	С	
60-64	C-	
55-59	D+	
50-54	D	
45-49	D-	
00-44	F	

ISACA (Information Systems Audit and Control Association). I encourage you to become student members of ISACA. Joining ISACA will provide access to a wealth of resources about the topics we cover in our class discussions. With student membership, you will gain access to articles in the Information Systems Control Journal, various IT audit & security toolkits, discounts on ISACA certifications (CISA, CISM), events, conferences, etc. Joining ISACA will also open the door to making connections with people around the globe who are currently working, and hiring for positions ranging from IT security, audit, control, risk, privacy, compliance, and advisory services. To learn more, please check out www.isaca.org/student.

KnowledgeLeader. I also encourage you to subscribe (free of charge) to Protiviti's KnowledgeLeader website. It provides audit programs, tools, resources and best practices to help busy professionals save time and stay current about business and technology risks. In addition, KnowledgeLeader offers the University Center for professors and students containing entry-level internal audit and risk management content and career resources. Complimentary accounts can be set up for this class.

McCombs Classroom Professionalism Policy

The highest professional standards are expected of all members of the McCombs community. The collective class reputation and the value of the Texas MPA experience hinges on this.

Faculty are expected to be professional and prepared to deliver value for each and every class session. Students are expected to be professional in all respects.

The Texas MPA classroom experience is enhanced when:

- **Students arrive on time.** On time arrival ensures that classes are able to start and finish at the scheduled time. On time arrival shows respect for both fellow students and faculty and it enhances learning by reducing avoidable distractions.
- **Students display their name cards.** This permits fellow students and faculty to learn names, enhancing opportunities for community building and evaluation of in-class contributions.
- **Students minimize unscheduled personal breaks.** The learning environment improves when disruptions are limited.
- **Students are fully prepared for each class.** Much of the learning in the Texas MPA program takes place during classroom discussions. When students are not prepared they

cannot contribute to the overall learning process. This affects not only the individual, but their peers who count on them, as well.

- **Students respect the views and opinions of their colleagues.** Disagreement and debate are encouraged. Intolerance for the views of others is unacceptable.
- **Laptops are closed and put away.** When students are surfing the web, responding to e-mail, instant messaging each other, and otherwise not devoting their full attention to the topic at hand they are doing themselves and their peers a major disservice.
- **Phones and wireless devices are turned off.** We've all heard the annoying ringing in the middle of a meeting. Not only is it not professional, it cuts off the flow of discussion when the search for the offender begins. When a true need to communicate with someone outside of class exists (e.g., for some medical need) please inform the professor prior to class.

Academic Dishonesty

I have no tolerance for acts of academic dishonesty. Such acts damage the reputation of the school and the degree and demean the honest efforts of the majority of students. The minimum penalty for an act of academic dishonesty will be a zero for that assignment or exam.

The responsibilities for both students and faculty with regard to the Honor System are described on http://www.mccombs.utexas.edu/MPA/Student-Code-of-Ethics.aspx. As the instructor for this course, I agree to observe all the faculty responsibilities described therein. During Orientation, you signed the Honor Code Pledge. In doing so, you agreed to observe all of the student responsibilities of the Honor Code. If the application of the Honor System to this class and its assignments is unclear in any way, it is your responsibility to ask me for clarification.

Students with Disabilities

Upon request, the University of Texas at Austin provides appropriate academic accommodations for qualified students with disabilities. Services for Students with Disabilities (SSD) is housed in the Office of the Dean of Students, located on the fourth floor of the Student Services Building. Information on how to register, downloadable forms, including guidelines for documentation, accommodation request letters, and releases of information are available online at http://deanofstudents.utexas.edu/ssd/index.php. Please do not hesitate to contact SSD at (512) 471-6259, VP: (512) 232-2937 or via e-mail if you have any questions.

COURSE OUTLINE

S#	Day	TOPIC	Reading / case assignments
1	Mon. June10	Introductions	Course syllabus
		Information Technology Environment & Security Pictor of The Medium Firms	GTAG-1: Information Technology Risk and Gaptrals and 2.25
		Risks of The Modern Firm By William Turner, PhD; Senior Director, Data Center Architecture, Presidio	Controls, pp. 2-25.
2	Wed.	COSO: A Framework For Enterprise Risk	COSO Executive Summary 2013
	June12	ManagementCOBIT: A Framework For Information	COBIT 5 Executive SummaryCOBIT 4.1 pages 9-28.
		Technology Risk Management	Caselet: Union National Bank
		Case-1: Data Theft at the McCombs School of	Case-1: Tanriverdi, H., Lau, S., Hubbard, H.,
		Business (2006)	Sukholutsky, D., and Liu, C. "Data Theft at the McCombs School of Business," The University of Texas at Austin, Austin, TX, 2007, pp. 2-10.
3	Mon. June17	Data Theft at the McCombs School of Business (2006) - Continued Discussion with David Burns, Director, Computer Support Services, McCombs Business School (via video link)	Reflect on discussions in the previous session and identify questions for David Burns.
		 IT Application Controls Audits IT General Control (ITGC) Audits 	 GTAG-8: Auditing Application Controls GAIT for IT General Control Deficiency Assessment - An approach for evaluating ITGC deficiencies in Sarbanes-Oxley Section 404 assessments of internal controls over financial reporting.
		Case-2: AlphaCo: A Teaching Case on Information Technology Audit and Security	 Case-2: Tanriverdi, H., Harrison, J., Mesuria, K.S., Bertsch, J., Hsiao, P., and Hendrawirawan, D. "AlphaCo: A Teaching Case on Information Technology Audit and Security," The Journal of Digital Forensics, Security and Law (1:1) 2006, pp 35-61.

S#	Day	TOPIC	Reading / case assignments
4	Wed. June19	Identity Governance & Access Controls By Collin Perry, SailPoint	GTAC-9: Identity and Access Management
		Case-3: Security breach at TJX Note: This is a required write-up case. Please submit your write-up by 1:30pm.	(HP) Case-3: Nicole R.D. Haggerty, Ramasastry Chandrasekhar. (2008). "SECURITY BREACH AT TJX." Richard Ivey School of Business. Version: (A) 2008-03-12
5	Mon. June24	Computer Aided Audit Tools & Techniques (CAATTS) and the Use of Data Analysis Please meet at MOD Lab at 1:30pm for a tutorial on ACL by course TA, Kui Du	 ACL Tutorial Notes by course TA, Kui Du CAATTS Assignment
		Auditing Privacy Controls By Michael Porier, Protiviti Please move back to regular classroom (UTC 4.122) at 3:15pm for this guest lecture	IPPF – Practice Guide - Auditing Privacy Risks
6	Wed. June26	The Changing Landscape of IT Regulations: Regulatory Compliance for Banking and Healthcare Industries By Brian Thomas & Reema Parappilly of Weaver	Reading assignment for the first guest lecture to be determined and posted on BB.
		IT Security Governance & Audits By Forrest Foster, Chief Security Architect, Cisco Systems	GTAG-15: Information Security Governance
7	Mon. July1	Payments Fraud, By Suba Vasudevan, Facebook	GTAG-13: Fraud Prevention and Detection in an Automated World
		Financial Audit Analytics By David Hendrawirawan, Dell	GTAG-16: Data Analysis Technologies

S#	Day	TOPIC	Reading / case assignments
8	Wed. July3	Digital Evidence & Computer Forensics By William Turner, PhD; Senior Director, Data Center Architecture, Presidio	Reading assignment for the guest lecture to be determined and posted on BB.
		Case-4: CHOICE POINT	• (HP) Case-4: Paine, L., and Phillips, Z. "Choice Point (A)," Harvard Business School Case #: 9-306-001, Boston, MA.
9	Mon. July8	Leveraging professional networks and certifications for a successful career in IT Audit & Internal Audit By ISACA and IIA Representatives (date to be confirmed)	Reading assignment for the guest lecture to be determined and posted on BB.
		IT Outsourcing Risks By Mark Envani, E&Y (date to be confirmed)	GTAG-7: Information Technology Outsourcing
10	Wed. Jul10	CAATTS assignments due by 1:30pm.	
	Juito	Addressing strategic IT risks and returns in corporate transactions such as mergers, acquisitions, spin-offs, split-ups	• Selim, G.M., Sudarsanam, S., and Lavine, M. "The role of internal auditors in mergers, acquisitions, and divestitures," International Journal of Auditing (7) 2003, pp 223-245.
		Course wrap-up	
		• Take home final given; solutions due by 5:30pm on July 13 th .	