THE UNIVERSITY OF TEXAS AT AUSTIN
ACC F380K 12 - COMPUTER AUDIT AND SYSTEM SECURITY
Summer 2020
Unique#: 71045

VERSION: 6/1/2020

Instructor	**:**	Hüseyin Tanriverdi
Class times	**:**	Monday / Wednesday 1:30-5:30 p.m.
Class location	**:**	Zoom
Instructor's Office	**:**	Zoom
Phone	**:**	(512) 232-9164
E-mail	**:**	Huseyin.Tanriverdi@mccombs.utexas.edu
Office Hours	**:**	By appointment
Teaching assistant	**:**	Kathryn Wargo kathrynwargo@utexas.edu

Course objectives:

This course makes an introduction to digital risks and risk mitigation mechanisms of organizations. Digital technologies have become a critical enabler and transformer of business innovation, growth, and profitability across almost all sectors of the economy. Digital technologies have also exposed organizations to risks such as cybersecurity risks, privacy risks, ethical dilemma risks in big data and analytics applications, and biases in machine learning and artificial intelligence algorithms. Such risks can affect the confidentiality, integrity, availability, and appropriate use of organization's information assets. They can lead to financial loss, reputational loss, and increased costs of regulatory compliance. Various laws, regulations, and industry standards require companies to institute internal control systems to mitigate such risks. The U.S. Securities and Exchange Commission (SEC) requires registrants to disclose information about their cybersecurity risks and incidents. Emerging new technologies such as Internet of Things (IoT), Artificial Intelligence (AI) and Machine Learning (ML), Robotic Process Automation (RPA), Blockchain, etc. offer new productivity, profitability, and transformation opportunities. They also create new cybersecurity and privacy risks, and new ethical, responsible design challenges. It is important for business leaders to understand how they can institute governance and control mechanisms to minimize such risks, maximize returns of digital technologies, and obtain favorable risk-return outcomes. This course aims to equip students with such skills and knowledge. The topics covered by the course include, but not limited to:

- Board of directors' and top management team's oversight of cyber risks, privacy risks, and ethical risks around digital technologies and algorithms
- Enterprise risk management and enterprise IT risk management frameworks
- IT general controls, IT application controls, identity governance and access controls, IT audit process, generally accepted IT audit standards and methodologies, and how they relate to financial audits
- Third-party risk management
- Organizational cybersecurity policies
- Organizational privacy policies
- Identity, security, privacy, and ethical dilemma implications of emerging information technology innovations (e.g., IoT, AI, ML, RPA, blockchain, etc.) and what they imply for the IT audit, security, and advisory services industry
- Algorithmic biases, adversarial attacks on machine learning and artificial intelligence algorithms, and governance and controls for mitigating such risks

- Fake news, mass digital surveillance by government and private enterprises, and manipulation of human behaviors

Course learning and delivery format:
The course uses a participant-centered, discussion-based, active learning format in which students share control and responsibility for learning. The course is delivered through live synchronous video sessions, using the Zoom technology. The course uses some lectures, a lot of interactive case discussions and analyses, and some guest lectures from the industry. Students will review the assigned readings, slide decks, and cases in advance of the class sessions, and use the synchronous video time to apply the learning to real life cases and clarify their questions. There will be a case discussion in each of the 10 sessions. We will use polls actively during discussions. Students are expected to read and analyze the assigned readings and cases in advance of class and come to class prepared to discuss the concepts, cases, and answer poll questions. By participating in class discussions and polls, students will control and share the responsibility for learning. The class is scheduled as a 4-hour class from 1:30pm to 5:30pm. To avoid "Zoom fatigue," I do not intend to use the full 4 hours on the Zoom screen. Instead, I will try to limit the Zoom time on any given class day to two 75 minute sessions with a 15 min. break in between. In the Zoom sessions, I will use some lecturing time to cover the most critical, difficult issues and address your questions. I will dedicate most of the Zoom time to the discussions and applications of the concepts in the readings to real life examples and case studies.

Course website:
Hosted on Canvas course management system: http://canvas.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 and they are marked with (HP) or (Canvas):

- **(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://hbsp.harvard.edu/import/730091
- **(Canvas)** Non-Harvard cases and readings will be posted on course website at Canvas: http://canvas.utexas.edu/

Grading

Contributions to in-class discussions	:	30%
Individual case write-ups	:	70%
Total	:	100%

Contributions to in-class discussions (30%). Students are expected to actively contribute to the learning of their peers by participating in class discussions and sharing their perspectives on issues being discussed. They are also expected to participate in Zoom polls actively. Class attendance is required, but it earns only 20% of the in-class participation credits. The remaining 80% of the in-class contribution credits can be earned by making contributions to in-class discussions, polls, and breakout groups.

There is no substitute or make-up for earning in-class contribution credits. Requests to do extra work in lieu of in-class contributions will be automatically declined. If you have to miss the opportunity to contribute to in-class discussions in a session, please try to make up for

it by increasing your contribution levels in the other sessions you are able to attend. Your final in-class contribution grade will be assigned based on your participation patterns throughout the semester.

Advanced preparation for in-class discussions is required to 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, polls, breakout groups, 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
- Keeping your video ON in Zoom with appropriate virtual background
- Participating in Zoom Polls
- Listening actively to your peers, instructor, and guest speakers
- Using Zoom controls appropriately (e.g., raise digital hand) to ask questions
- Unmuting yourself to respond to questions directed to you
- 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
- Disagreeing with others constructively
- Neither dominating the conversations nor being too quiet
- Exhibiting a good sense of humor and professional Zoom etiquette

Individual case write-ups (70%): We will discuss a total of 10 cases throughout the semester. You are required to submit write-ups for any five of them. You are welcome to submit a 6th case write-up to substitute the lowest case grade. The weighted average of the top five case write-up grades will make up 70% of the final grade. Cases are weighted equally. Case write-up questions will be posted on the assignments sections of the course website on Canvas. Format, submission, and grading guidelines are posted on Files\Case write-up guidelines section of Canvas. Your case analysis and write-up should address the assigned questions posted on Canvas by utilizing course concepts covered in reading assignments, lectures, and analyzing the facts and evidence in the case studies. The managerial issues entailed in the cases are open ended. They can potentially be analyzed and addressed in multiple different ways. Case write-ups are INDIVIDUAL assignments. You should analyze the 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. The case write-ups are due on Canvas by the beginning of class, i.e., 1:30pm, on the day of the case discussion. Submissions after this deadline will not be considered. There will be no make up for a missed write-up as we already offer a total of 10 case write-up opportunities. Before you develop a case write-up, please do the assigned readings of the case day and reflect on the course concepts covered to date to decide which concepts are most relevant for developing your perspective on the case questions.

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	A
90-94	A-
85-89	B+
80-84	B
75-79	B-
70-74	C+
65-69	C
60-64	C-
55-59	D+
50-54	D
45-49	D-
00-44	F

Format of online classes: we aim to do online classes *synchronously* through live video and audio features of Zoom. Please set up Zoom and follow the guidance provided by UT / McCombs: https://wikis.utexas.edu/display/MSBTech/Getting+Started+With+Zoom

Zoom skills: If you have not already, please learn how to use Zoom and get ready for online classes. If you need help with Zoom, please refer to the McCombs Student Instructional Resources Wiki. All Canvas webpages for all McCombs courses will have a link to the McCombs Student Instructional Resource Wiki on the bottom left corner, so students can access it from their Canvas course pages.

Preferred method of joining a class or office hours in Zoom: The preferred method of joining a class or office hours is through video on Canvas. Students must log into their Canvas course site and click on Zoom in the left toolbar to locate links to join the class in Zoom.

Zoom etiquette: Here are some best practices for making sure we are working together to create an efficient, effective, respectful, and ultimately enjoyable classroom.

- **Arrive in advance.** Plan to arrive in an online class at least five minutes in advance of the class start time, i.e. by 1:25pm the latest for our class. You will need a few minutes to register for a session, and test your audio, video, and other settings. We will start the class at 1:30pm sharp. For security reasons, I will follow the university's recommendation to lock the Zoom meeting at 1:30pm sharp to prevent Zoombombing attacks or other inappropriate use by unauthorized parties.
- **Mute yourself.** You will be automatically muted upon entry to a Zoom session in our class. Keep yourself muted until you are called on or you would like to speak. This will cut down on background noise and limit any distractions.
- **Keep your camera ON**. We aim to create a virtual class environment where we can see each other live. Please keep your camera ON at all times during a class session.

- **Avoid messy / inappropriate background.** If your room or background is messy or if it is not appropriate for a professional meeting, use Zoom's Virtual Background feature to introduce a professional background. Be mindful of your surroundings on camera. We want to make sure we avoid as much distraction as possible.
- **Add profile photo.** Please add a professional photo of yourself for your Zoom profile picture. This photo will be visible if you have to turn off your video.
- **Avoid / minimize going in and out of class.** As in a regular classroom, try not to leave the virtual class room unless it is absolutely necessary. Going in and out of class is disruptive to other participants. If you absolutely have to leave the online class temporarily, please use the away feedback icon and temporarily turn your camera off.
- **Digitally raise your hand to get the air.** Use the digital "Raise Hand" button in the "Participants" menu of Zoom to alert the instructor that you would like to have the air. Speak when the instructor gives you the air. Try to keep questions and comments brief. With a large classroom, be cognizant that there are many people to get through and many questions to move through.
- **Go slower / faster.** If you feel that the class is moving too fast or too slow, use the "go slower" / "go faster" icons on the "Participants" menu to alert the instructor.
- **Video/audio quality.** If the video or audio quality at your end is choppy, use the "Chat" menu to alert the instructor about the problem. Try to temporarily turn off your video to address the problem.
- **Internet connection.** Please try to use a reliable WIFI connection.

Class recording privacy: You should not record the Zoom sessions on your local computer. To the extent that guest speakers give permission, instructor will record the sessions and make them available on Canvas. Such class recordings are reserved only for student use in this class for educational purposes. The recordings should not be shared outside the class in any form. The University's policy is to process the violations of these restrictions as part of Student Misconduct policies.

Help from Student Emergency Services: Students who need help getting access to technology in order to do online instruction should fill out the Student Emergency Services form. For general inquiries, please contact Student Emergency Services.

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.

Religious holy days. By UT Austin policy, you must notify me of your pending absence at least fourteen days prior to the date of observance of a religious holy day. If you must miss a class, an examination, a work assignment, or a project in order to observe a religious holy day, you will be given an opportunity to complete the missed work within a reasonable time after the absence.

COURSE OUTLINE

- Readings marked with **(Canvas)** are to be posted on course website on http://canvas.utexas.edu/
- Readings marked with **(HP)** are available in a digital course package at Harvard: https://hbsp.harvard.edu/import/730091

S#	Date	Topic	Readings/Assignments
1	M 6/8	▪ Introductions ▪ **Cybersecurity risks and cyber risk oversight**	• (Canvas) Course syllabus • (Canvas) What boards are doing today to better oversee cyber risk. E&Y 2019.
		▪ **Enterprise risk management:** COSO Framework ▪ **Case-1:** McCombs Data Theft	• (Canvas) Galligan, M.E. and Rau, K. (2016). "COSO in the Cyber Age" pp. 1-18 • (Canvas) Case-1: Tanriverdi, H., Lau, S., Hubbard, H., 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.
2	W 6/10	▪ **Enterprise cyber risk management:** NIST Cybersecurity Framework	• (Canvas) NIST Cybersecurity Framework V.1.1., 2018.
		▪ **IT controls and regulatory compliance:** e.g., Sarbanes-Oxley (SOX) Act Section 404 ▪ **Case-2:** AlphaCo case	▪ (Canvas) Protiviti. (2012). Guide to the Sarbanes-Oxley Act: IT Risks and Controls. ▪ (Canvas) 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.
3	M 6/15	• **Third-Party Vendor Risks** • **System & Organization Controls (SOC)** By Mark Knight, Partner & Joey LoSurdo, Partner, Holtzman Partners	• (Canvas) On the Road to SOC 2 Readiness. Protiviti.
		• **Case-3:** Data Breach at Equifax	• (HP) Case-3: Srinivasan, S., and Pitcher, Q. (2017). "Data Breach at Equifax." Harvard Business School, pp. 1-15.
4	W 6/17	• **Robotic Process Automation** By Alex Phillips and Calvin Witt, Protiviti	• (HP) Lacity, M.C., and Willcocks, L.P. (2016). "A New Approach to Automating Services." MIT Sloan Management Review, SMR571-PDF-ENG.

S#	Date	Topic	Readings/Assignments
		• **Risk/Return of Robotic Process Automation** • **Case-4:** Osara	• (HP) Case-4: Kerr, W.R., Palano, J., and Huang, B. (2019). "Osaro: Picking the best path." Harvard Business School, 820012-PDF-ENG.
5	M 6/22	• **Corporate Identity and Access Management** By Collin Perry, Principal, Cybersecurity & Privacy, PwC	• (Canvas) Identity and Access Management Guide, SailPoint.
		• **Identity Theft** • **Case-5:** Who is this guy?	• (Canvas) Ethical decision making frameworks (also see https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/) • (HP) Case-5: Brannen, D.E., Medcalfe, S.K., and Cousins, R.B. (2015). "Who is this guy?" North American Case Research Association.
6	W 6/24	• **Algorithmic bias risks**	• (Canvas). Lee, N.T., Resnick, P., and Barton, G. (2019). "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms." The Brookings Institution.
		• **Risk/Return of AI in Human Resource Management** • **Case-6:** GROW360	• (HP) Case-6: Bernstein, E.S., McKinnon, P.D., and Yarabe, P. "GROW: Using Artificial Intelligence to Screen Human Intelligence." Harvard Business School, 418020-PDF-ENG.
7	M 6/29	• **Blockchain**	• (Canvas) Jehl, L.E., and Bartish, B. (2018). "Blockchain 'Smart Contracts' – A New Transactional Framework." Baker & Hostetler LLP, pp. 1-3. • (Canvas). KcKinsey. (2018). "Blockchain beyond the hype: What is the strategic business value."

S#	Date	Topic	Readings/Assignments
		• **Case-7:** RegTech at HSBC	• (HP) Case-7: Dey, A., Heese, J., Weber, J. (2019). "Regtech at HSBC." 120046-PDF-ENG. • RegTech Universe 2020. Deloitte. • https://youtu.be/YsBPkVC5gJ0 • https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html
8	W 7/1	• **Organizational Privacy Policies** By Luis Castillo and Justin Turner, Protiviti	• (Canvas) NIST Privacy Framework V.1.0, 2020.
		• **Risk/Return of AI in Health Care Assistants** • **Case-8:** Amazon Alexa and Patient Engagement	• (HP) Case-8: Schulman, K.A., Wood, S. (2019). "Amazon Alexa and Patient Engagement." SM328-PDF-ENG.
9	M 7/6	• **Organizational Cybersecurity Policies**	• (Canvas) A Board's Guide to the NIST Cybersecurity Framework for Better Risk Oversight. PwC. 2019.
		• **Security versus Privacy** • **Case-9:** Apple	• (HP) Case-9: Jayakumar, T. and Tahora, S. (2017). "Building a Backdoor to the iPhone: An Ethical Dilemma." Ivey Publishing, W16245-PDF-ENG.
10	W 7/8	• **Surveillance capitalism**	• (Canvas) Zuboff, S. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* (30:1), pp. 75-89.
		• **Case-10:** Facebook	• (HP) Case-10: Yoffie, D.B., Fisher, D. "Fixing Facebook: Fake News, Privacy, and Platform Governance." Harvard Business School Case #: 720400-PDF-ENG.