ITP-471 "Consultancy Skills for Cyber Security Risk Management"
Units: 4
Term: Spring
T TH TBD

Location: TBD

Instructor: Gregg Ibbotson

Office: RRB 221
Office Hours:
    By Appointment
Contact Info:
    Ibbotson@usc.edu

IT Help: Viterbi IT

Hours of Service:
    Monday – Friday, 8:30 a.m. – 5:00 p.m.
Contact Info:
    DRB 205
    (213) 740-0517
    engrhelp@usc.edu

Course Description

Consultancy Skills for Cyber Security Risk Management focuses on developing your teambuilding and communication skills to be an effective leader in consulting. It will explore key cyber security frameworks such as the ISO 27001 security standard and NIST, as well as skills relevant to being a consultant. The ISO 27001 is a globally recognized standard for the implementation of cyber security controls. It empowers organizations to apply a systematic approach to cyber incident response and cyber risk management. The course will cover the planning and implementation of an ISMS (information security management system) in alignment with ISO 27001 and other reputable standards from NIST. It will focus on the development of auditing skills and procedures, such as interview techniques and audit report writing. The course will have a comprehensive case study, linked to all seminars and homework to further facilitate this development.

Catalog Description
Working through the ISO27001 Cyber Security Standard. Developing consultancy skills by conducting cyber risk assessments, policy evaluations, and project team development tailored to business objectives.

Learning Objectives

By the end of the course, students will:
- Navigate and interpret cyber frameworks including: the ISO 27001 Standard and several key NIST standards
- Recognize the business needs for cyber security and be able to tailor a suitable solution
- Apply and justify appropriate security controls to mediate the business issues of the case study
- Articulate requirements of the standards to a variety of different business role audiences
- Conduct a stage 1 audit (fundamental requirement auditing i.e in ISO 27001)
  - Produce an audit agenda
  - Interview staff
- Develop a comprehensive audit report (stage 2 audit) to the format expected by businesses

Prerequisite(s): ITP 125
Co-Requisite(s): none
Concurrent Enrollment: NA
Recommended Preparation: NA

Course Notes

Lecture slides and course content, including homework, will be posted to the course Blackboard page. Course announcements will be posted as an announcement to Blackboard or emailed directly to your USC emails

Technological Proficiency and Hardware/Software Required

Basic familiarity with Google Slides or PowerPoint

USC Technology Support Links
https://keepteaching.usc.edu/start-learning/
https://studentblackboardhelp.usc.edu/
https://software.usc.edu/

Syllabus for **ITP-471**

Required Readings and Supplementary Materials

Digital copies of ISO 27001, ISO 27002 and ISO 19011 to be provided
NIST Risk Management Framework https://csrc.nist.gov/Projects/risk-management/about-rmf

Description and Assessment of Assignments

Security control allocation assignments (3x 5%)
Throughout the course, students will be given mini-scenarios (a few sentences to explain a given business practice) and will be expected to suggest an appropriate set of ISO 27001 Annex A controls or Clauses to mitigate the given issue. There will be three of these in total – 5% each.

For example: "Sarah and Cameron were overheard sharing login details for a secure database system. Cameron explained that his manager gave him a last-minute deadline for some system checks, and that he only has 48 hours to complete them. He states that the I.T approval request could probably take longer than two days to sort out, so he has no choice but to borrow Sarah's"

Audit interview prep (5%)
To produce a list of open-style questions aimed to assess the needs of different members within the organization case study. Namely the CEO and those involved in the creation of the company's risk assessment process
You may wish to split the clauses up for each team member to focus on. 6 Questions.
List your clause next to your questions.

Live Interview session (5% - participation)
The aforementioned questions will be asked in class in a live environment in the form a role-playing session. Answers they receive may form new lines of questioning and it is expected students react appropriately

Audit schedule for stage 1 (5%)
Students will produce an audit schedule and scope statement based on how they feel will best address the needs of the case study organization. This will be a detailed version of the in-class activity 5 from week 3.

Stage 1 Audit Report (10%)
Working in teams, prepare a stage 1 audit report, no more than 4 pages (including the title page)

3 nonconformity reports (3x5%)
To produce 3 nonconformity reports in the format required by ISO 27001 to outline the remedial action required to meet the needs of the controls/clause of the case study. A template will be provided.
The case study will be based on a fictional I.T services company. Students will be given the company's ISMS (information security management) documentation to review throughout the classes.

Risk Management Group Report (10%)
Following up on your stage 1 audit report, the CEO Samantha has acknowledged the risk management method of her ISMS has some areas to improve on. Your task is to re-write it.

Risk Management Group Presentation (5%)
Present a proposal of your updated risk method to the CEO (5%)

Syllabus for **ITP-471**

Final Project – Auditor Guidebook (total 30%)
You are a lead auditor and have been asked to write a simple guidebook for a new junior member of staff, Alice, as she is about to embark on her first-ever audit. This will allow you to consolidate all the class concepts, and present it in an easily approachable manner to an inexperienced auditor.

Assignment Breakdown

Assignment	% of grade
Security control allocation assignments (x3)	15
Audit interview prep	5
Live Interview session (Participation)	5
Audit schedule for stage 1	5
Stage 1 Audit Report	10
3 nonconformity reports (5% each)	15
Risk Management group report	10
Risk Management group presentation (participation)	5
Final Project (Auditor Guidebook)	30
TOTAL	**100**

Assignment Rubrics
Full detailed grading schemes will be available for students to view at the start of the course

Assignment Submission Policy
All homework assignments will be submitted via Blackboard. Assignments submitted via email will not be accepted. The exception is the live interview session which will be done in class in real-time

Additional Policies
The only acceptable excuses for missing an assignment deadline or taking an incomplete in the course are personal illness or a family emergency. Students must inform the instructors/administration staff before the assignment due date and present verifiable evidence for a deadline extension to be granted.

If you know you will be missing any classes at the beginning of the semester, please tell the instructor as soon as possible.

Synchronous session recording notice
During remote teaching situations, the Zoom courses will be recorded, and these recordings will be shared with the class. While this will not entirely replace in-class participation, these recorded classes will allow students to catch up on lectures they were unable to attend as well as for useful review.

Course Schedule: A Weekly Breakdown

Purple: Graded homework Black: non-graded in-class activities

Week	Topics/Daily Activities	Readings and Homework	Deliverable/Due Dates
1	**Operational Enterprise Cybersecurity** Cyber Projects / frameworks / architecture (advanced)	Download the ISO 27001 standard and **briefly** summarize the 10 clauses	Due Monday of week 2 (not graded – class discussion)
2	**Cybersecurity frameworks and standards** Understanding the organization and its context and management obligations. Planning for ISMS evaluation.	Read over the NIST Risk Management Framework (RMF). **Prepare for Security control allocation assignment No1**	Analysis due end of week 3
3	**The Role of an Auditor** Core competencies and interview methods. Planning the Audit team. Stage 1 and 2 audits	**Prepare for Security control allocation assignment No2**	Analysis due end of week 4
4	**Preparing for ISMS evaluation.** Developing work documents and checklists. Opening Meetings.	**Prepare for Security control allocation assignment No3**	Analysis due end of week 5
5	**Developing consultancy skills** Communication Skills Audit reports	Read over Auditor competencies in the ISO 19011 standard. Active Listening activities **Create a stage 1 audit schedule**	Schedule due end of week 6
6	**Establishing the consultancy team** Creating interview questions	**Create interview questions**	Interview questions are due Monday of week 7 Interviews will take place during the class of week 7
7	**Conducting interviews (senior management)** **Conducting interviews (Operational staff)** **Deliver questions in class.**		Analysis due end of week 9
8	**User training process and measuring competence** Tools selection and implementation	**Produce Stage one audit report**	Report due start of week 13
9	**Physical Security** The importance of physical security/staff training	Document physical security controls and implementation methods in line with the case study. Group quiz **Produce Stage one audit report**	Review in class
10	**Spring Break! Woooooo!**		
11	**User Training**		
12	**Evaluating non-conformities** Performing an in-depth document review of the case study	**Work on nonconformity reports**	Reports due end of week 14
13	**Advanced Cyber Risk Management (Planning and Implementation)** Project planning and design Implementation related to ISO 27001 and NIST frameworks	**Work on Risk Management Report**	Reports due end of week 15
14	**Advanced Cyber Risk Management (Planning and Implementation)** Project planning and design Implementation related to ISO 27001 and NIST frameworks		
15	**Staff interview's part 2 – risk management follow-up** **Presentations**	**Work on Risk Management Presentation**	Due in class week 15
16	**Cyber Insurance and Project Management** **Audit stage 1 and Stage 2 Review session** Students will start work on their final projects in class. A class discussion will be had on whether we would recommend the case study organization for certification.	**Work on the final project**	
Final	**Final Project submission**		USC Exam period

Syllabus for **ITP-471**

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in SCampus in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

Support Systems:

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL), press "0" after hours – 24/7 on call
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED) - (213) 740-5086 | Title IX – (213) 821-8298
equity.usc.edu, titleix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office of Equity and Diversity |Title IX for appropriate investigation, supportive measures, and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

USC Campus Support and Intervention - (213) 821-4710
campussupport.usc.edu
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity at USC - (213) 740-2101
diversity.usc.edu
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call
dps.usc.edu
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
ombuds.usc.edu
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.