USC Viterbi
School of Engineering
Information Technology Program

ITP 370: Information Security Management
Units: 3
Term: Spring 2022
TBD

Location: TBD

Instructor: Gregg Ibbotson

Office: RRB 221
Office Hours:

Contact Info:
ibbotson@usc.edu

Teaching Assistant: TBD

Office: TBD
Office Hours:
TBD
Contact Info:
TBD

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

Last updated: 11/17/21

Course Description

To develop your understanding and awareness of industry focused processes and implementation techniques for cyber security. The course covers flexible, scalable methodologies and frameworks that you can use to tailor solutions to a given business. The course begins with how to understand the needs of a business, perform a gap analysis and develop a series of cyber security recommendations, from a procedural standpoint. These recommendations are to be based from a fictional case study organization.

These methods and flexible approaches will enable you to provide a critical link between the requirements and operational business needs of an organization, and the cyber security systems needed to protect them. This course covers a range of key topics to prepare you for future career, such compliance, GDPR, Cyber Risk Management, Cyber incident response and communication skills.

Catalogue Description
Cybersecurity project design. Incident response. Teambuilding, management and communications for cybersecurity. Scalable approaches for implementation of Information Security Management Systems.

Learning Objectives

Upon completing this course, students will:

- Gain substantial, practical experience in planning and implementing standard-based information security management systems to meet the requirements of large organizations
- Gain experience of and expertise in developing procedures, policy documentation and other controls required for the management of information security
- Understand the fundamentals of information security management
- Understand the key concepts of cyber frameworks and compliance
- Understand the importance of asset management and system benchmarking
- Develop competent knowledge of Cyber Risk Management and Incident Response procedures
- Develop communication and presentation skills

Prerequisite(s): none
Co-Requisite(s): none
Concurrent Enrollment: none
Recommended Preparation: none required

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

It is assumed that the student has baseline technical knowledge (basic computer usage, basic internet usage). For any upper-division course (300-level and above), it is assumed that you have refined your technical abilities in ITP 125

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

https://software.usc.edu/

Required Readings and Supplementary Materials

All course materials will be posted on Blackboard - http://blackboard.usc.edu
Readings exist in the syllabus

Description and Assessment of Assignments

Note: The assignments will be based off of a fictional case study
This will be based on a fictional I.T services company. Students will be given a 12-month incident report detailing passed incidents, along with financials and organizational structure.
There will also be key staff listed in which the students will be able to interview via role playing activities during the course.

1. **Homework: Developing an Information Security Management System for the course case study (50%)**

This will involve performing extensive research into the practices necessary to mitigate the risks associated with the case study. The output from this should take the form of a plan for the creation of an Information Security Management System (ISMS). The key areas and their associated percentages are given below.

1. Obligation and Scope (5%) Due end of week 3

2. Asset Management (10%) Due end of week 5

3. Risk Assessment (20%) Due end of week 9
    - Risk Methodology
    - Risk Identification
    - Risk evaluation
    - Risk Treatment

4. Incident management Procedure (10%) Due end of week 13

5. Gantt Chart (5%) Due end of week 15

2. **Interview sessions 10%** Due end of week 4
   To produce a list of open style questions for key staff in the case study, to perform a gap analysis

3. **Final Project (40%)** Due end of week 15
   Policy design and Implementation. The importance and structure of Policy's is paramount to this report. At a policy level, controls need to be discussed with a more **managerial tone** rather than technical. The detail comes in the procedures. There are several incidents in the case study, so justification for content for each policy / procedure focusing on how those incidents would be covered is needed to demonstrate understanding.
    1. Policies, standards, processes and procedures. You need to demonstrate you understand the differences between them and their intended audience (5%)
    2. **List** a set of 3 polices, justify why they have been selected (e.g. in relation to the case study) for each document and briefly justify why. (15%)

3. Create 2 of your chosen 3 policies, and 1 procedure relevant to the case study (total 10%)
    - Produce 2 polices (5% each)
    - 1 procedure to match up with one of your polices (5%)

4. To present to members of the case study team your proposal of changes (10%) – exam period

Grading Breakdown

Assignment	% of grade
Homework: Developing an Information Security Management System for the course case study (50%)	50%
Interview sessions	10%
Final Project	40%
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

Week	Topics/Daily Activities	Readings and Homework	Deliverable/Due Dates
1	Introduction to Information Security Management (ISM) and Security Development Life Cycle (SDLC)	na	na
2	Introduction to Frameworks and compliance	Homework 1: Obligation and scope	Due end if week 3
3	Contingency Planning	Create a business impact analysis table. Prepare interview questions	Due end of week 4
4	Cyber Asset Management	Homework 2. Asset Management	Analysis due end of week 5
5	**Interview sessions**	As above	As above
6	Performance Metrics and Benchmarking	Create a performance measurement document for your chosen security program	In class
7	Introduction to Cyber Risk Management	Homework 3. Design a Risk Management Procedure for the case study	Analysis due end of week 9
8	Introduction to Security Polices	Final Project	Project due end of week 15
9	Project Management	Produce Gantt Chart	Due end of week 15
10	Intro to Cyber Incident Response part 1	na	na
11	Intro to Cyber Incident Response part 2	Homework 4. Produce an Incident Management Procedure	Due end of week 13
12	Data Privacy and regulations	na	na
13	GDPR PCI-DSS CPRA and IoT security	Na	na
14	Portfolio prep		
15	**Presentations**		

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.