USC Viterbi
School of Engineering
*Information Technology Program*

**ITP 370: Cyber Security Management and Operations**
**Units:** 4
**Term: Fall 2023**
T TH 11-12:50

**Location:** See Schedule of classes

**Instructor:** Gregg Ibbotson

**Office:** RRB 221
**Office Hours:**

**Contact Info:**
ibbotson@usc.edu

**Teaching Assistant:** TBD

**Office:** zoom
**Office Hours:**
TBD
**Contact Info:**
TBD
Live interview Participation
**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:** 8/17/23

**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 on 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 a future career, such as 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:

- Utilize a mixture of cyber frameworks and in-class practical sessions to implement standard-based information security management systems to meet the requirements of large organizations
- Produce a series of information security policies and procedures to satisfy the requirements of the assignment case study
- Create custom asset and risk registers to practice security control selection, bolstering the maturity level of the case study organization
- Apply the fundamentals of information security management and frameworks to reduce the likelihood of future cyber attacks
- Carry out cyber control benchmarking activities to evaluate their own cyber control recommendations, against that of the current state of the assignment case study.
- Develop competent knowledge of Cyber Risk Management and Incident Response procedures
- Develop communication and presentation skills

**Prerequisite(s):** itp 125
**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

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

**Required Readings and Supplementary Materials**

No textbook for the course is required.

**Description and Assessment of Assignments. Note: The assignments will be based** off **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 past 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 (45%)**
   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 (non-homework in class activity)
   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 13

2. **Interview sessions (5%)** Due before the class of week 5
   To produce a list of open-style questions for key staff in the case study, to perform a gap analysis

3. **Consulting 1 to 1 interview (5%)**
   In interactive mock interview training session to prepare you for work in one of the big consulting firms.

4. **End of course Presentation (5%)**
   To present to members of the case study team (via role play) your proposal of changes
   During week 15, you will be given a new mini case study. You will work in **new** groups of 4 to create and deliver a presentation in the form of a PowerPoint. This will take place during class.
   Your group will present to the CEO and CISO of this company the proposed upgrades to their security and justification of those upgrades.
   9-minute presentation + 5 minute Q&A with the company representatives.
   Recommendations must have real products with real prices - give at least 2 options for each category.
   A recommendation-focused presentation including policy recommendations when appropriate.
   Remember to engage and relate to your audience.
   Your group can decide how to break up the workload, so long as there is a fair contribution from all group members.

5. **Final Project (40%)** Due during the **finals exam period**. This is a written report, 3500 words.

   **Executive Summary (5%)**
   The start of the report must begin with an **executive summary**. While it is the first part the reader sees; it is usually the last part to be written.
   This is aimed at the management and director level of Shameless and must cover an overview of the purpose of the ISMS, key areas of concern (in particular your risk register), and legal requirements. This must be no more than 1 page (500 words)

   **Policy Design and Implementation (35%).** The importance and structure of policies 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 the 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. Please detail and give examples of these 4 different document types (750 words) (5%)
   2. **List** a set of 3 policies, 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 (750 words each) relevant to the case study (total 15%)
      - Produce 2 policies (5% each)
      - 1 procedure to match up with one of your policies (5%)

**Grading Breakdown**

| Assignment | % Of grade |
|---|---|
| | |
| Homework: Developing an Information Security Management System for the course case study | 45% |
| Interview sessions | 5% |
| Consulting 1 to 1 interview | 5% |
| Presentation | 5% |
| Final Project | 40% |
| **Total** | **100%** |

**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.
Late assignments docked 25% after 24 hours, 50% after 48 hours, and not accepted after 72 hours.

**Grading Policies**
The instructors will do their best to return assignments graded to students within 2 weeks of the submission. Certain assignments that are longer in length like final projects, may require more time.

**Additional Policies**
The only acceptable excuses for missing an assignment deadline or taking an incomplete in the course are documented illness or emergency, which can include email communication between a student and instructor

## Course Schedule: A Weekly Breakdown

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

| Week | Topics/Daily Activities | Readings and Homework | Deliverable/Due Dates |
|---|---|---|---|
| **1** | Introduction to Information Security Management (ISM) and Security Development Life Cycle (SDLC) Governance | Review the Shameless consulting case study | - |
| **2** | Introduction to Frameworks and Compliance | Obligation and scope | Due end of week 3 |
| **3** | Contingency Planning | Create a Business Impact Analysis (BIA) table<br>Prepare interview questions | Questions due end of week 4 |
| **4** | Cyber Asset Management | Homework 1. Asset Management | Due end of week 5 |
| **5** | Interview sessions | - | - |
| **6** | Performance Metrics and Benchmarking | Create a performance measurement document for your chosen security program | In class |
| **7** | Introduction to Cyber Risk Management | Homework 2. Design a Risk Management Procedure for the case study | Due end of week 9 |
| **8** | Cyber risk evaluation and treatment | As above | as above |
| **9** | Project Management | Produce Gantt Chart | Due end of week 13 |
| **10** | Consulting 1 to 1 Activity | | |
| **11** | Intro to Cyber Incident Response p1 | Final Project released | **USC finals exam period** |
| **12** | Intro to Cyber Incident Response p2. Log Management | Homework 4. Produce an Incident Management Procedure | Due end of week 13 |
| **13** | Introduction to Security Policies and User training<br>Consultancy Presentation Preparation | - | - |
| **14** | Tuesday - Presentations<br><br>**Thursday - Thanksgiving** | - | - |
| **15** | Data Privacy and regulations (GDPR PCI-DSS CPRA and IoT security)<br>Follow up Interview session.<br><br>Consulting Careers discussion | | |
| **Finals** | **Final project submission** | | **USC finals exam period** |

**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. 1.16.2020

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.