Syllabus: INFSYS 3878/6878

Information Security Risk Management & Business Continuity

About this course:

**Required texts:**

You will not need to purchase a text book or any other materials for this course. We will be using a range of open source materials freely available online.

- Considerable material in the form of notes, PowerPoint slides, and web links will be assigned and available through Canvas.
- Suggested (but not required) books for further reading:

**Other course materials:** As assigned by instructor

Materials used in this course are “affordable or open educational resources” (A/OER), which means they are available at low or no cost to students. These openly licensed quality resources selected by your instructor are used in order to save you money and provide access to all of the course content on day one of this course.

**Time Requirements:**

If this course were offered on campus, you’d be in class 2.5 hours/week plus travel time. The online version is no different in terms of expectations for your involvement. This is an active online course that requires 3 hours of your time each week in addition to the time it takes you to read the required materials, watch the videos, and complete the assignments. That means that you need to plan to spend a minimum of 6 hours every week (up to 9-10 hours a week) on activities related to this course. If you are worried about your preparedness, consider taking the [Online Readiness Survey](#) to help decide if an online course is right for you.

**Technology Requirements:**

As a student in an online course, you are expected to have reliable internet access almost every day. If you have computing problems, it is your responsibility to address these or to use campus computing labs. Problems with your computer or other technology issues are not an excuse for delays in meeting expectations and missed deadlines for the course. If you have a problem, get help in solving it immediately. At a minimum, you will need the following software/hardware to participate in this course:

1. Computer with an updated operating system (e.g. Windows, Mac, Linux)
2. Updated Internet browsers (Apple Safari, Internet Explorer, Google Chrome, Mozilla Firefox)
3. Ability to navigate Canvas (Learning Management System)
4. Minimum Processor Speed of 1 GHz or higher recommended.
5. DSL or Cable Internet connection or a connection speed no less than 6 Mbps.
6. Media player such as VLC Media Player.
7. Adobe Flash player (free)
Course Description

**Prerequisites:** INFSYS 3848 or Consent of Instructor. This course provides students the tools and concepts necessary to plan for, prevent, and when needed successfully respond to disruptions in business operations. Topics covered include security policies, frameworks, information and materials management, risk management, and regulatory compliance. Credit cannot be granted for both INFSYS 3878 and INFSYS 6878.

**Goals of the Course:**
Upon completion of the course, students will have a basic understanding of at least the following:

- The need for systematically managing InfoSec
- InfoSec Governance
  - Obtaining and maintaining top management commitment
  - InfoSec Strategy and its alignment with IT and Business Strategies
  - Establishing and Maintaining a governance framework to support all InfoSec activities
  - Security planning including business continuity in the face of breaches
  - Policy formulation
  - Identifying stakeholders and assigning roles and responsibilities
  - Initiating processes to establish, record, and evaluate “security metrics”
- Risk Based Management of InfoSec including
  - Identifying information assets and their associated security requirements
  - Establishing risk criteria
  - Risk analysis and risk evaluation
  - Risk treatment
    - security controls
  - InfoSec security management standards/models (and the organizations that develop these)
- Incident handling and response
  - Processes to identify breaches in security
  - Creating processes to streamline reporting of breaches internally and externally
  - Processes to mitigate security breaches in accordance with organizational planning for security contingencies
- Regulatory compliance and ethics
  - Understanding how regulation and ethical norms shape organizational management of InfoSec

**How to Succeed in This Course**

The course is divided into 16 weekly modules. Each module will open on Saturday and all assignments will be due **BY 8:00 PM** the following Sunday. We will utilize discussion boards, writing assignments, 2 exams and one project. If you keep up with the material, lectures and discussions, you will have a good chance for success.
Information Security Risk Management & Business Continuity

Assessment/Grading

Grade Composition:
During the course of the semester, exams, and assignments will be given and managed via Canvas. The total points available during the semester will be 750. Letter grades will be given as follows:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>750-675</td>
</tr>
<tr>
<td>B</td>
<td>674-600</td>
</tr>
<tr>
<td>C</td>
<td>599-525</td>
</tr>
<tr>
<td>D</td>
<td>524-450</td>
</tr>
<tr>
<td>F</td>
<td>0-449</td>
</tr>
</tbody>
</table>

The point distribution breaks down as follows:

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>POINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project</td>
<td>100</td>
</tr>
<tr>
<td>In-term Exam</td>
<td>100</td>
</tr>
<tr>
<td>Final Exam</td>
<td>100</td>
</tr>
<tr>
<td>Quizzes/Assignment/Discussions</td>
<td>320</td>
</tr>
<tr>
<td>NICE Challenges</td>
<td>130</td>
</tr>
<tr>
<td>Total</td>
<td>750</td>
</tr>
</tbody>
</table>

At the instructor’s discretion, there may be additional extra credit assignments made throughout the semester.

Grading Scale: The UMSL Grading System is based on a four-point scale. The grade value for each letter grade is as follows:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>4.0</td>
</tr>
<tr>
<td>A-</td>
<td>3.7</td>
</tr>
<tr>
<td>B+</td>
<td>3.3</td>
</tr>
<tr>
<td>B</td>
<td>3.0</td>
</tr>
<tr>
<td>B-</td>
<td>2.7</td>
</tr>
<tr>
<td>C+</td>
<td>2.3</td>
</tr>
<tr>
<td>C</td>
<td>2.0</td>
</tr>
<tr>
<td>C-</td>
<td>1.7</td>
</tr>
<tr>
<td>D+</td>
<td>1.3</td>
</tr>
<tr>
<td>D</td>
<td>1.0</td>
</tr>
<tr>
<td>D-</td>
<td>0.7</td>
</tr>
<tr>
<td>EX</td>
<td></td>
</tr>
<tr>
<td>DL</td>
<td></td>
</tr>
<tr>
<td>FN</td>
<td></td>
</tr>
</tbody>
</table>

Feedback and Grading Timeline:
Grades for projects and exams will be posted within 1 week following the due date under normal circumstances. You can find your grade in the Grades button on Canvas. Quiz grades will be available upon completion. If there is a rubric attached to the assignment or discussion board, you can click your score to see my personal feedback on the rubric.

Late assignments will not be accepted for credit without consent from the instructor prior to the due date.
Online Discussion Rubric  
(Two Criteria)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Exceeds Expectations</th>
<th>Meets Expectations</th>
<th>Developing Need for Improvement</th>
<th>Missing</th>
</tr>
</thead>
</table>
| **Original Post** | 6 pts.  
Use of analysis, synthesis and evaluation  
Critical and/or creative contribution  
Incorporates readings well into responses, demonstrating excellent understanding.  
Asks questions that extend the discussion and relate material to prior course content.  
Makes insightful, critical comments on the readings and to fellow students.  
Contributes new information and identifies the source. | 4 pts.  
Use of comprehension and application  
Incorporates readings into responses, demonstrating solid understanding.  
Exhibits some insights and understanding of course content, but may not ask critical questions of the readings or fellow students.  
May relate module’s issues to prior material covered in the course.  
May respond to fellow students. | 2 pts.  
Use of knowledge  
Repeats basic correct information related to discussion, but neglects to extend conversation or critically analyze course content. | 1 pt.  
No clear evidence that readings were understood or even completed.  
0 pts.  
No postings throughout the week |
| **Reply(ies)/Question to Classmate** | 4 pts.  
Insightful question or reply to a classmate’s post. Asks questions that extend the discussion and makes insightful, critical comments. | 3 pts.  
Exhibits good insights and understanding of discussion questions. | 2 pts.  
Repeat basic correct information related to discussion. | 1 pt.  
Only agreed/disagreed but never contributed to the ongoing conversation.  
0pts.  
Did not reply or question any classmates. |
# Course Schedule (subject to modification)

<table>
<thead>
<tr>
<th>Week of</th>
<th>Module / Name</th>
<th>Readings</th>
<th>Assignments</th>
<th>Due Date</th>
</tr>
</thead>
</table>
|         | Course Introduction & syllabus review | NIST 800-53 Revision 4 Pages: 1-13  
CMU Governing for Enterprise Security Implementation Guide Pages: 1-14 | Introduce Yourself  
Discussion Board | Risk Analysis 1 |
|         | InfoSec strategy, alignment with organizational goals, roles and responsibilities within the organization. | PCI-DSS 3.1 Requirement 12 (pages 100-110)  
SANS Policy Templates (for further reference) | Discussion Board | Risk Analysis 2 |
|         | InfoSec governance framework | AFCEA – Economics of Cyber Security  
CMU: The ROI of Security PODCAST  
CMU: The ROI of Security TRANSCRIPT | Discussion Board | Risk Analysis 3 |
|         | Developing business cases for security investments.  
Developing InfoSec metrics | NIST 800-39 Pages 1-32  
Three ROI articles: Schneier on Security (archive)  
Security Week (archive)  
Lenny Zeltzer (archive) | Discussion Board | NICE Challenge |
|         | Risk analysis financial impact. Quantitative vs. qualitative,  
Total Cost of Ownership, Risk Analysis Matrix | PCI-DSS 3.1 Requirements 2.4, 9.7, 11.1, 11.2, 11.3, 12.3  
NIST 800-30 Revision 1 Pages: 4-38 | Discussion Board | Risk Analysis 4 |
|         | Managing risk assessments, vulnerability assessments and penetration tests | FAIR Introduction  
FAIR Basic Risk Assessment Guide | Discussion Board | Risk Analysis 5 |
Center for Internet Security Critical Security Controls Controls 1, 2, 20  
NIST 800-30 Revision 1 | Discussion Board | Risk Analysis 6 |
<table>
<thead>
<tr>
<th>Topic</th>
<th>Pages: 4-38</th>
<th>Discussion Board</th>
<th>Midterm Exam</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal, regulatory and contractual compliance.</td>
<td>CSO Online Law/Reg Directory (Note that there are four pages to this article.) Microsoft: Understanding Regulatory Compliance (archive) Educause (archive) HHS HIPAA Summary (archive) AMA HIPAA Overview (archive)</td>
<td>Discussion Board</td>
<td>Midterm Exam</td>
</tr>
<tr>
<td>Midterm exam</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InfoSec awareness and education programs Aligning InfoSec with other business units (HR, Legal, etc.)</td>
<td>PCI DSS Best Practices for Implementing a Security Awareness Program PCI DSS v2.0 Best Practices for Maintaining PCI DSS Compliance Section 3.8 Security Awareness Training is a Waste of Time (archive) Security Awareness Training is a Cost Effective Control (archive) NIST 800-50</td>
<td>Discussion Board</td>
<td>NICE Challenge</td>
</tr>
<tr>
<td>InfoSec when dealing with external partners SOC compliance/auditing</td>
<td>Combatting Cyber Risks Supply Chain PCI DSS Third Party Security Assurance</td>
<td>Discussion Board</td>
<td>Risk Analysis 7</td>
</tr>
<tr>
<td>Integrating information security into business and IT processes</td>
<td>MITRE Cyber Security Governance Pgs 1-20</td>
<td>Discussion Board</td>
<td>Risk Analysis 8</td>
</tr>
</tbody>
</table>
## Course Policies

**Participation (expectations)**

- It is vitally important that our classroom environment promote the respectful exchange of ideas. This entails being sensitive to the views and beliefs expressed during discussions whether in class or online. Please speak with me before recording any class activity. It is a violation of University of Missouri policy to distribute such recordings without my authorization and the permission of others who are recorded.
- I will monitor each discussion but will not respond to each post.
Your success in this course will heavily depend on your ability to communicate, engage and participate in all course activities. Successful completion of this course requires that a student keep up with all assignments, coursework and discussions. Timely participation in online discussions is a very important part of this course and participation in these discussions, and other activities as assigned, is not optional. You are expected to prepare and post to discussions in a timely manner consistent with the requirements contained within the course syllabus and discussion rubric*.

If you are unable to participate in the scheduled class activity or discussions, you must notify the instructor within the week of that class module or discussion. An unexcused failure to engage or participate with the class will be counted as an absence; unexcused absences may result in failure. The instructor reserves the right to make judgment to accept and/or make–up assignments missed because of failed participation in the course activities.

Online Discussion Protocol

- Participation in the course should maintain a positive work and learning environment, as outlined in the UM Collected Rules & Regulations, 330.080
- Postings should be evenly distributed during the discussion week.
- Postings should be a minimum of three sentences, or one short paragraph, and a maximum of two paragraphs.
- Responses should be well written with proper punctuation, spelling and grammar.
- Avoid short one-word postings, for instance, “I agree,” unless accompanied by supporting statements from the readings or prior knowledge (work and life experience).
- Stay focused on the topic.
- Ask questions; challenge other postings that lack supporting evidence or present incorrect information.
- Encourage further discussion by building on current threads.
- Check your postings for responses from others and respond in kind.
- Use proper “netiquette”.

Attendance Policies

- Present in class for online courses is determined by participation in an “academically related activity,” i.e. submission of an assignment, assessment or discussion forum posting. The last day of attendance is the last day a student is academically participating in the online course.
- Documentation that a student has logged into an online class is not sufficient by itself to demonstrate academic attendance.

Academic Integrity/Plagiarism

- You are responsible for being attentive to and observant of University policies about academic honesty as stated in the University’s Campus Policies and Code of Student Conduct found in the UMSL Bulletin
  - Academic dishonesty is a serious offense that may lead to probation, suspension, or dismissal from the University. One form of academic dishonesty is plagiarism – the use of an author’s ideas, statements, or approaches without crediting the source. Academic dishonesty also includes such acts
Syllabus: INFSYS 3878/6878

Information Security Risk Management & Business Continuity

as cheating by using any unauthorized sources of information and providing or receiving unauthorized assistance on any form of academic work or engaging in any behavior specifically prohibited by the faculty member (e.g., copying someone else’s answers on tests and quizzes). Unauthorized possession or distribution of academic materials is another type of academic misconduct. It includes the unauthorized use, selling or purchasing of examinations or other academic work, using or stealing another student’s work, unauthorized entry or use of material in a computer file, and using information from or possessing exams that an instructor did not authorize for release to students. Falsification is any untruth, either verbal or written, in one’s academic work. Facilitation is knowingly assisting another to commit an act of academic misconduct. Plagiarism, cheating, and falsification are not acceptable.

○ All instances of academic dishonesty will be reported to the Office of Academic Affairs who will determine whether you will appear before the Student Conduct Committee for possible administrative sanctions such as dismissal from the university. The instructor will make an academic judgment about the student’s grade on that work in this course. The campus process regarding academic dishonesty is described in the “Policies” section of the Academic Affairs website.

Title IX Policies

In adherence to the policies of Title IX and to promote a safe and secure educational environment, it is strongly recommended statements similar to those below be added to your course syllabus:

• Mandatory Reporting: Under Title IX, all UMSL faculty, staff, and administrators (with limited exception) are obligated to report any incidents of sexual harassment, sexual misconduct, sexual assault, or gender discrimination to the Student Affairs office and/or other University officials. This ensures that all parties are protected from further abuses and that victim(s) are supported by trained counselors and professionals. Note: There are several offices at UMSL (e.g., Counseling Services, Health Services, Community Psychological Service, Center for Trauma Recovery, and Student Social Services) whose staff are exempt from Title IX mandated reporting, when the information is learned in the course of a confidential communication.

Technical Support

Online Mentor Program

Online education requires different teaching, learning, and technology skills than those found in traditional face-to-face classes. We assist students with the online technology in Canvas and provide resources for studying and success in online classes.

• 598 Lucas Hall
• Phone: (314) 516-4211
• Email: onlinementor@umsl.edu
• Website: http://www.umsl.edu/services/ctl/studentsupport/omp.html
Canvas
If you have problems logging into your online course, or an issue within the course site, please contact the Technology Support Center:
- Phone: (314) 516-6034
- Email: helpdesk@umsl.edu
- Website: http://www.umsl.edu/technology/tsc/

If you are having difficulty with a technology tool in Canvas, consider visiting the Canvas Student Guides, which has overviews of each tool and tutorials on how to use them.

If you continue to experience problems or just have questions, you can also contact the Learning Resource Lab:
- Phone: (314) 516-6704
- Email: lrl@umsl.edu
- Website: http://www.umsl.edu/technology/lrl/

VoiceThread
- Online Contact Form: https://voicethread.com/support/contact/
- Website: https://voicethread.com/howto/

Student Resources

Access, Disability and Communication
Your academic success is important. If you have a documented disability that may have an impact upon your work in this class, please contact Disability Access Services (DAS) immediately. Students must provide documentation of their disability to the office of Disability Access Services in order to receive official University services and accommodations. The staff is available to answer questions regarding accommodations or assist you in your pursuit of accommodations. Information about your disability is confidential. Once DAS reviews your medical documentation, they will provide you with the information and steps to inform me about the accommodations to which you are entitled. Your accommodations will begin as soon as we discuss your approved accommodations.
- 144 Millennium Student Center (MSC)
- Phone: (314) 516-6554
- Email: Tara Cramer, cramert@umsl.edu
- Website: http://www.umsl.edu/services/disability/

Office of International Students and Scholar Services
If you have difficulty communicating in English with the instructor of this course, contact ISS.
- 362 Social Sciences & Business Building (SSB)
- Phone: (314) 516-5229
- Email: iss@umsl.edu
- Website: http://www.umsl.edu/~intelstu/contact.html
Syllabus: INFSYS 3878/6878

Information Security Risk Management & Business Continuity

Student Enrichment and Achievement

SEA provides comprehensive support and intervention strategies that support your road to graduation!

- 107 Lucas Hall
- Phone: (314) 516-5300
- Email: umselsea@umsl.edu
- Website: https://www.umsl.edu/services/sea/

Office of Multicultural Student Services (MSS) and the University Tutoring Center (UTC)

MSS provides comprehensive student retention services to diverse student populations; through their tutoring center, the MSS offers comprehensive tutoring services free to students at UMSL.

- 225 Millennium Student Center (MSC)
- Phone: (314) 516-6807
- Email: multicultural@umsl.edu
- Website: https://www.umsl.edu/~mcraa/index.html

More Student Resources are on the Learning Resource Lab website.

Online Class Netiquette/Behavior

- **Be self-reflective** before you post an emotional response and reread what you have written to be sure it is positive. Think of your comments as printed in the newspaper. Your online comments will be seen, heard and remembered by others in the class.

- **Use effective communication.**
  - Avoid the use of all caps or multiple punctuation elements (!!!, ??? etc).
  - Be polite, understate rather than overstate your point, and use positive language.
  - If you are using acronyms, jargon or uncommon terms, be sure to explain them so everyone can understand and participate in the discussion.

- **Ask for clarification** to a point if you feel emotional from a classmate’s post. It is likely that you misunderstood his/her point. This strategy will also help you step away from the intensity of the moment to allow for more reflection.

- **Sign your name.** It is easier to build a classroom community when you know to whom you are responding.

- **Foster community.** Share your great ideas and contribute to ongoing discussions. Consider each comment you make as one that is adding to, or detracting from, a positive learning environment for you and your classmates.

- **Be constructive.** You can challenge ideas and the course content, but avoid becoming negative online. When you disagree politely, you stimulate and encourage great discussion. You also maintain positive relationships with others with whom you may disagree on a certain point.
Information Security Risk Management & Business Continuity

• **Keep the conversation on topic** by responding to questions, adding thoughtful comments about the topics at hand. Online dialogue is like conversation. If there is a certain dialogue going on, please add to it, but if you have something new to say, please post it in another thread.

• **Define your terms.** When using acronyms or terms that are particular to your field (or new to our course), please define them for others.