ISM 4323 - INFORMATION SECURITY AND IT RISK MANAGEMENT

SYLLABUS

Room	: BSN 115	**Meetings**:	T, TH 3:30 – 4:45 pm
Instructor	: Stephen Sebesta		
Office	: LSA 114		
Telephone	: (813)-974-8126		
E-mail	: ssebesta@usf.edu		
Office Hours	: Hour before class or by appointment		
Textbook	:http://www.wiley.com/WileyCDA/WileyTitle/productCd-EHEP003131.html?filter=TEXTBOOK		
Readings	: http//www.ismlab.usf.edu/isec		
Resources	: ftp://ftp.usf.edu/pub/ism/InfoSec_Linux_VM_012017.ova		
Pre-requisites	: Interest in computers and information security		

Course objectives

The goal of the course is to introduce skills and knowledge on Information Security and IT Risk Management in businesses. The course is open to students in all majors. Course objectives will be accomplished through two categories of information – (1) helping students develop technical skills to secure computer networks by implementing IT general controls and (2) introducing frameworks that comply with legal provisions for the assessment of IT risk in a business environment.

The course will include class presentations and extensive hands-on projects on implementing the common IT controls such as access control lists (ACLs), firewalls, network scanning, STIG (Security Technical Implementation Guidelines), identifying software errors and documenting some key IT General Controls. Required reports will help students improve their writing and documentation skills.

A good class combines teaching a trade and thinking about the trade. This class has an approximately 40-60 balance between skills acquisition and conceptual understanding.

Specifically, the course objectives are:

1. To introduce the importance of information security and related business concern.
2. To make students aware of the major categories of information security threats.
3. To make students aware of the common information security controls.
4. To enable students to implement the basic information security controls.
5. To introduce students to the important legal provisions regarding information security.
6. To make students aware of the methodological implications for information security arising from these legal provisions.
7. To provide students with an understanding of the standard methodologies for complying with legal requirements for IT general controls.
8. To provide basic understanding of IT risk management in organizations.

The student learning outcomes are:

1. Students will demonstrate an understanding of security concerns and issues in organizations.

2. Students will have the ability to identify major categories of information security threat.
3. Students will have the ability to apply various kinds of controls to counter common threats
4. Students will have the ability to apply best practices related to IT controls to comply with legal requirements.
5. Students will have the ability to provide solutions to mitigate IT risks.

Logistics

1. Students may form groups of three students each to complete projects.
2. Use the phrase "ISM4323" in the subject line of your email (no spaces) to help me filter emails.
3. In all deliverables and communication, please include the names of ALL students involved. This is needed for allocating grades correctly. **You will lose credit for not doing so**.
4. Readings and assignment deliverables are always scheduled on the Friday of the week.
5. Deliverables are due by the end of day on the due date (usually this means 11:55pm).
6. Make up opportunities will only be provided for job-related situations and for medical emergencies in the immediate family.
7. Assignments for each chapter have 5 components – questions, example case, critical thinking, hands-on activities and design case. Critical thinking and example case are worth 0.5% each, the other activities are worth 1% of the credit for the course. These assignments can take time, please plan your time accordingly.
8. We will try to manage class time so that as much of the hands-on activity is performed in class as possible.
9. The design case is your opportunity to conduct industry research. This is your opportunity to discover issues, concerns, products and solutions not discussed in class and apply them within a coherent framework to solve customer concerns.
10. I will do my best to try and teach you something useful, not merely certify what you already know. This impacts exam preparation for example, where you should not expect a shortlist of questions to prepare.
11. Subject to availability of time, select groups will be invited to present their designs in class on the last day.

ISACA Essay Competition (TENTATIVE)

The Information Systems Audit and Control Association (Wiki) is sponsoring an essay competition for students in this class. All students will be required to submit an essay for class credit (3-5%), due at the end of the second week in April (tbd). Students may also request to have their essay submitted to the competition for scholarships.

1st Place: $1,000
2nd Place: $500
3rd Place: $250

Additionally, 10 free ISACA Student Memberships will be awarded to interested students. There is an awards ceremony tentatively scheduled in November; more information will be released during the semester.

Potential topics include:

- Cyber threats/risks (e.g., HeartBleed Bug)
- Cyber security management/trends
- Cloud computing security
- Data privacy management/security
- Social media security
- New technology security (such as Google Glass)
- Third Party Vendor Management and Risk
- The Internet of things (IoT)

*Other topics are allowed but must be relevant and approved before submission.

Highly recommended resources on Information Security and IT Risk Management

If you have anything more than a passing interest in information security and IT risk management, the following books cannot be recommended enough. Information from all these sources is used in the class. The Anderson book provides detailed managerial coverage of information security problems and solutions. The Mandia book has recipes for responding to intrusions. Perlman's book has an extra-ordinarily great presentation of encryption algorithms. Westerman's book describes why IT risk management deserves top-management attention and how the major IT risks can be identified.

1. Anderson, Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 20 02, ISBN 0-471-38922-6
2. Incident Response and Computer Forensics, Second Edition, by Chris Prosise, Kevin Mandia and Matt Pepe, McGraw-Hill/Osborne; 2 edition (July 17, 2003), ISBN: 007222696X
3. Kaufman, Charlie, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a P ublic World. 2nd ed. 2002: Prentice-Hall
4. Westerman, George and Richard Hunter, IT Risk: Turning Business Threats into Competitive Advantag e (Hardcover). 2007, Boston, MA: Harvard Business School press

Business Continuity

In the event of an emergency, USF may opt to continue delivery of instruction through methods that include but are not limited to: Blackboard, Elluminate, Skype, and email messaging and/or an alternate schedule. It's the responsibility of the student to monitor Blackboard for each class for course specific communication, and the main USF, College, and department websites, emails, and MoBull messages for important general information.

Grading

Activity	Type	Unit weight	Total weight
Assignments	Group	4%	56%
Quizzes	Individual	5%	15%
Design presentation	Group	5%	5%
ISACA	Individual	3%	3%
Exam	Individual	20%	20%

Grading policy

Total%	**Grade**	**Total%**	**Grade**	**Total%**	**Grade**	**Total%**	**Grade**
>= 95	A+ (max 10% of class)[1]	>= 85	B+	>= 75	C+	>= 65	D+
>= 90	A	>= 80	B	>= 70	C	<= 60	D
>= 88	A-	>= 78	B-	>= 67	C-	< 60	F

[1] At instructor's discretion

ISM 4323 - Tentative course outline*

Week	Topic	Readings	Assessments	Deadlines***	Other deadlines
1	Syllabus, Introduction	Chapter 1		Create groups	
2	Introduction	Chapter 1	Quiz 1 (ch 1) [5%]****		
3	System administration – part 1, 2	Chapter 2		Chapter 1 [4%]	
4	System administration – part 1, 2	Chapter 3		Chapter 2 [4%]	
5	Basic information security model	Chapter 4		Chapter 3 [4%]	
6	Asset identification	Chapter 5		Chapter 4 [4%]	
7	Threats and vulnerabilities	Chapter 6	Quiz 2 (ch 2 – 5) [5%]	Chapter 5 [4%]	
8	Encryption controls	Chapter 7		Chapter 6 [4%]	ISACA Essay
9	Identity & access management	Chapter 8		Chapter 7 [4%]	
10	Hardware and software controls	Chapter 9		Chapter 8 [4%]	
11	Shell scripting	Chapter 10	Quiz 3 (ch 6 - 9) [5%]	Chapter 9 [4%]	
12	Incident handling	Chapter 11		Chapter 10 [4%]	
13	Incident analysis	Chapter 12		Chapter 11 [4%]	
14	Policies	Chapter 13		Chapter 12 [4%]	Design case presentation [5%]
15	Risk analysis and management	Chapter 14		Chapter 13 [4%] Chapter 14 [4%]	
15 – 16	Exam [20%]				

*In the interests of the class, deviations may be made in the coverage of topics as outlined in the tentative course calendar. However, to help plan your calendars for the rest of the semester, assessment and deadline dates will be non-negotiable after the first day of class.